

**STRAYER UNIVERSITY**

**ASSESSMENT OF TECHNOLOGIES  
FOR FORENSIC AUDITING  
TO COMBAT MONEY LAUNDERING  
IN THE U.S. BANKING INDUSTRY**

**A DIRECTED STUDY PROJECT SUBMITTED TO THE  
FACULTY OF THE GRADUATE SCHOOL OF BUSINESS  
IN CANDIDACY FOR THE DEGREE OF  
MASTERS OF SCIENCE IN PROFESSIONAL ACCOUNTING**

**BY**

**PETER CLARK**

**DECEMBER 1999**

**DISTRIBUTION STATEMENT A**  
Approved for Public Release  
Distribution Unlimited

**DTIC QUALITY INSPECTED 1**

**20000223 033**

REPORT DOCUMENTATION PAGE			Form Approved OPM No. 0704-0188	
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction searching existing data sources gathering and maintaining the data needed, and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Report, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503.</small>				
1. AGENCY ONLY (Leave Blank)		2. REPORT DATE 17 December 1999		3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE  Assessment of Technologies for Forensic Auditing to Combat Money Laundering in the U.S. Banking Industry			5. FUNDING NUMBERS  N/A	
6. AUTHORS  Peter Clark				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)  N/A			8. PERFORMING ORGANIZATION REPORT NUMBER  N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)  N/A			10. 9. SPONSORING/MONITORING AGENCY REPORT NUMBER  N/A	
11. SUPPLEMENTARY NOTES  This report was a directed study project submitted to the faculty of the graduate school of business in candidacy for the degree of masters of science in professional accounting, Strayer University.				
12a. DISIRIBUTION/AVAILABILITY STATEMENT  Approved for public release; Distribution is unlimited.			12b. DISTRIBUTION CODE  A	
13. ABSTRACT (Maximum 200 words)  This paper analyses the recommendations of six money laundering investigation and detection experts. The insertion of newly identified technologies, and auditing practices to detect and deter money laundering in the banking industry were explored to support these recommendations. The experts rank-ordered responses to a listing of contemporary research findings on technology from a government-appointed panel on money laundering investigation and prosecution. They also provided open-ended responses to questions about applying information technology to assist auditors in the banking industry with money-laundering detection. This study found high congruence among the experts for the development and application of at least two of the proposed technologies. Further, they endorsed the role and application of other technologies not reviewed by the government panel. A case was made for the importance of the bank auditor's role, and to interact in a complementary fashion with the expert systems. This study suggests, and concurs with findings of several other recent studies that information technology coupled with the enhanced capabilities of auditors provides a critical asset to money laundering detection. The Project DrugMARKET Interim Final Report was used as a springboard for this report.				
14. SUBJECT TERMS Drugs; Drug Trafficking; Financial Crimes; Law Enforcement; Money Laundering; Research & Development; Technology			15. NUMBER OF PAGES 76	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

## **ABSTRACT**

This paper analyses the recommendations of six money laundering investigation and detection experts. The insertion of newly identified technologies, and auditing practices to detect and deter money laundering in the banking industry were explored to support these recommendations. The experts rank-ordered responses to a listing of contemporary research findings on technology from a government-appointed panel on money laundering investigation and prosecution. They also provided open-ended responses to questions about applying information technology to assist auditors in the banking industry with money-laundering detection. This study found high congruence among the experts for the development and application of at least two of the proposed technologies. Further, they endorsed the role and application of other technologies not reviewed by the government panel. A case was made for the importance of the bank auditor's role, and to interact in a complementary fashion with the expert systems. This study suggests, and concurs with findings of several other recent studies that information technology coupled with the enhanced capabilities of auditors provides a critical asset to money laundering detection.

## TABLE OF CONTENTS

<b>Chapter</b>	<b>Page</b>
<b>1. INTRODUCTION</b>	<b>1</b>
<b>Context of the Problem</b>	<b>1</b>
<b>Statement of the Problem</b>	<b>4</b>
<b>Significance of the Study</b>	<b>7</b>
<b>Objectives of the Study</b>	<b>7</b>
<b>Review of the Literature</b>	<b>8</b>
<b>Research Methodology</b>	<b>9</b>
<b>Sources</b>	<b>10</b>
<b>2. INTERNAL CONTROL</b>	<b>11</b>
<b>Background</b>	<b>11</b>
<b>Research Process</b>	<b>19</b>
<b>Findings</b>	<b>20</b>
<b>Implications and Recommendations</b>	<b>24</b>
<b>3. TECHNOLOGY</b>	<b>25</b>
<b>Background</b>	<b>25</b>
<b>Research Process</b>	<b>32</b>
<b>Findings</b>	<b>34</b>
<b>Implications and Recommendations</b>	<b>40</b>

<b>4.</b>	<b>EXPERT SYSTEMS</b>	<b>41</b>
	<b>Background</b>	<b>41</b>
	<b>Research Process</b>	<b>50</b>
	<b>Findings</b>	<b>50</b>
	<b>Implications and Recommendations</b>	<b>53</b>
<b>5.</b>	<b>SUMMARY AND CONCLUSIONS</b>	<b>54</b>
	<b>Summary</b>	<b>54</b>
	<b>Conclusions</b>	<b>56</b>
	 <b>ABBREVIATIONS</b>	 <b>58</b>
	<b>APPENDIX A: DRUGMARKET PROJECT DESCRIPTIONS</b>	<b>61</b>
	<b>APPENDIX B: INTERVIEW QUESTIONNAIRE</b>	<b>67</b>
	<b>APPENDIX C: RESPONDENTS</b>	<b>69</b>
	<b>BIBLIOGRAPHY</b>	<b>70</b>

## ILLUSTRATIONS AND TABLES

### ILLUSTRATIONS

Figure	Page
1. Civil Penalty Annual Workload and Number of Civil Penalty Cases Closed (1985 - 1997) . . . . .	21
2. Average Processing Time for Civil Penalty Cases That Were Closed (1985 - 1997) . . . . .	21

### TABLES

Table	
1. Comparison of Internal Control (IC) Concepts	24
2. Technologies to Assist Law Enforcement	35
3. Technologies to Assist Auditors	35

# CHAPTER 1

## INTRODUCTION

### Context of the Problem

Money laundering is defined as, "the process whereby proceeds, reasonably believed to have been derived from criminal activity, are transported, transferred, transformed, converted, or intermingled with legitimate funds, for the purpose of concealing or disguising the true nature, source, disposition, movement or ownership of these proceeds".<sup>1</sup> Drug trafficking, prostitution, terrorism, arms trafficking, kidnapping,<sup>2</sup> and various other financial crimes generate enormous cash flows that create profiles which could bring about suspicion to the criminal organization. These criminals need first to conceal the existence of their ill-gotten funds, then disguise the funds as legitimate so that they can be used freely. To do this, the criminal must somehow move these illegal proceeds into the global financial system. The challenge to the criminal offender is to avoid attracting the unwanted attention of the Internal Revenue Service (IRS) and other law enforcement agencies involved in searching out illegal funds and hence causing damage to the organization. Along with moving cash out of the country and depositing it in a foreign bank operating under less stringent banking laws, bribing a bank manager, or discretely purchasing real estate or personal property, the classic approach is for a courier to deposit cash with a bank. To avoid the \$10,000 reporting requirement under the Bank

---

<sup>1</sup> U.S. Customs Service, quoted in Phil Williams, *Criminal Organizations: Money Laundering*, (Chicago, University of Chicago), 10, n. 4, (1995) 2.

<sup>2</sup> Many governmental reports cite these examples as collateral dimensions of money laundering activity. Note: Terrorism, unlike the other crimes mentioned, is usually not for financial gain. Terrorists may smuggle or wire money into this (or other) countries to support their activities and like the other money launders, they wish to conceal both the origin and the destination of their funds.

Secrecy Act (BSA)<sup>3</sup>, hundreds of couriers (or "smurfs"<sup>4</sup> as they are called) would scatter among the banks throughout the United States with deposits under \$10,000. This serious loophole under the BSA, allows for limitless variables: use of multiple banks, branch offices, teller stations, financial instruments, accounts, and individual deposits on any given day, in depositing illegal money. In 1986, the Money Control Act (MCA)<sup>5</sup> attempted to close the loopholes in prior laws that allow the "structuring" of transactions to flourish. In criminalizing the structuring of transactions (making several deposits/withdrawals under \$10,000) to avoid the reporting requirement of the BSA, the U.S. Congress attempted to inconvenience criminals by no longer allowing banks to accept suit cases or trash bags of cash unquestioned. Under the new law, employees of financial institutions must file a Currency Transaction Report (CTR) if they have knowledge that an attempt at structuring has occurred. Thus, it appeared as if the ability to launder the profits from illegal activities would be severely hampered.<sup>6</sup> This however, has not been the case.<sup>7</sup> Recent law enforcement estimates are that over \$100 billion is laundered annually in the United States and over \$500 billion worldwide.<sup>8</sup> The State Department's 1998 International Narcotics Control Strategy Report noted concern that new banking practices, such as direct access banking which permits customers to process

---

<sup>3</sup> The BSA obligates financial institutions to report cash transactions in excess of \$10,000 using the Currency Transaction Report (CTR) and requires individuals to report the transportation of currency in excess of \$10,000 into or out of the U.S.

<sup>4</sup> Couriers who move from bank to bank conducting multiple cash transactions under the \$10,000 reporting limit. The name "smurf" comes from the hyperactive blue cartoon characters.

<sup>5</sup> The MCA declared money laundering to be a federal crime and made "structuring" transactions to avoid filing a CTR a criminal offense.

<sup>6</sup> Bortne, Mark. *"Cyberlaundering: Anonymous Digital Cash and Money Laundering"*, Class Presentation, University of Miami, 1996, 1

<sup>7</sup> Banks maintain that stopping the placement of "dirty" cash through the teller's window is a top priority. However, they also acknowledge, that most money laundering passes through their automated systems and that these transactions are difficult to detect.

<sup>8</sup> Ehlers, Scott. *"In Focus: Drug Trafficking and Money Laundering"*, A Project of the Institute for Policy Studies and Interhemispheric Resource Center, Vol. 3, No. 16 (June 1998): 1

transactions directly through their accounts by computer operating on software provided by the bank, limit the ability of the banks to monitor account activity.<sup>9</sup>

The following example illustrates common money laundering practices and the difficulty of detection. "Mr. Big" Drug Dealer is the leader of an ongoing narcotics ring. He has rooms filled with currency, representing the profits from his illegal business activities. He needs to enter this cash into the legitimate, mainstream economy so that he can use these funds freely to purchase needed supplies, fund street dealers, purchase real or personal property and earn legitimate returns on the funds. All of these financial goals could be accomplished without a bank account, but efficiency demands legality. "Mr. Big" employs Larry Launderer<sup>10</sup> to "wash" the "dirty" funds. Larry then employs his vast army of smurfs to deposit currency under different names in amounts between \$7,500 and \$8,500 at branches of every bank within the region. Deposits are repeated twice a week for as long as is required. Meanwhile, Larry has been transferring the deposited funds from each bank branch, making withdrawals only once a week, and depositing the money into legitimate accounts controlled by "Mr. Big" at Internet banks that accept cyber-cash.<sup>11</sup> To be safe, Larry has these transfers limited to a maximum of \$8,000 each. Once the hard cash has been converted into digital cyber-cash, the illegal funds have become

---

<sup>9</sup> U.S. Department of State., International Narcotics Control Strategy Report, 1998., Bureau for International Narcotics and Law Enforcement Affairs, *"Money Laundering and Financial Crimes"* : Washington, DC, 2.

<sup>10</sup> In most cases, the actual money launderer is not an employee of the organization, but a contractor serving several drug dealers. Many of these individuals are paid as much as 20% for laundering money, fronting the drug dealers as little as 80% and then assuming the risk of cleaning the money.

<sup>11</sup> Cyber-cash and smart cards are an electronic replacement for "hard" cash. They hold a series of numbers that have intrinsic value in some form of currency.

virtually untraceable. "Mr. Big" now has access to legitimate and "clean" funds.<sup>12</sup>

### **Statement of the Problem**

In testimony before the House Committee on Banking and Financial Services, Jonathan Winer, then the Deputy Assistant Secretary, Bureau for International Narcotics and Law Enforcement Affairs, Department of State, reported:

"money laundering has devastating social consequences and is a threat to national security because it provides the fuel [for] . . . criminals to operate and expand their criminal enterprises. In doing so, criminals manipulate financial systems in the United States and abroad. Unchecked, money laundering can erode the integrity of a nation's financial institutions."<sup>13</sup>

Financial institutions continue to be both the witting and unwitting participants in money laundering operations because they are such easy targets: cash intensive businesses that provide a variety of services and instruments (cashier's checks, traveler's checks, and wire transfers) that can be used to conceal the sources of money. Wire transfer systems have become the method of choice allowing criminal organizations, legitimate businesses and individual banking customers to enjoy a swift and nearly risk-free conduit for moving money between countries. It is estimated that 700,000 wire transfers occur daily in the United States, moving well over \$2 trillion.<sup>14</sup> Thus, illegal funds can be easily hidden among legitimate fund transfers.

When financial transactions were posted by hand, auditors could visually observe each transaction. Today, however, because of the use of computers, auditors can no

---

<sup>12</sup> Bortne, 3.

<sup>13</sup> Testimony of Jonathan Winer, Deputy Assistant Secretary Bureau for International Narcotics and Law Enforcement Affairs, House Committee on Banking and Financial Services, *"Combating Money Laundering"*, Washington, DC, (June 1998): 3

longer visually inspect posted transactions, not only because of the sheer volume, but because computers are performing all accounting activities in real-time. Lastly, the average auditors' knowledge in information technology has not kept pace with the exponential growth in the advancement of the technology, especially in terms of on-line real-time global 24-hour access.<sup>15</sup>

The perennial theme of international, national and regional money laundering conferences attended by financial, policy and law enforcement professionals has been to increase the role and application of information technology to fight money laundering. In recognition of this, the Department of Defense (DoD) Counterdrug Technology Development Program Office (CDTDPO)<sup>16</sup> appointed a panel of experts in 1998 to study the information handling and processing challenges to money laundering investigators, focusing on information technology (IT) tools and methodologies. This study known as Project DrugMARKET (Drug Money Analysis, Research and Knowledge Engineering Task) was to baseline the state-of-the-art in money laundering investigation capabilities of the field investigator and the prosecutor and to recommend where new technology can improve the investigation process. Panelists interviewed money laundering experts (i.e., field investigators from different law enforcement agencies) and visited several large money laundering task forces under the auspices of High Intensity Drug Trafficking

---

<sup>14</sup> U.S. Congress, Office of Technology Assessment, *Information Technologies for Office Control of Money Laundering*, OTA-ITC-630, (Washington, DC: U.S. Government Printing Office, (September 1995): iii

<sup>15</sup> Respondent No. 2: Principal Investigator/FACFE (See APPENDIX C: RESPONDENTS).

<sup>16</sup> CDTDPO is a research and development organization for DoD. It manages and directs selected basic and applied research & development (R&D) technology prototype projects for DoD elements that are supporting the enforcement of anti-drug laws as well as drug law enforcement agencies.

Areas (HIDTAs)<sup>17</sup>. Its objective was to discover what works and what does not, and how investigations could be conducted better, faster, and cheaper.<sup>18</sup> Particular emphasis was placed on the increasing importance of combined federal and state investigative initiatives and tools and strategies for more effective casework. The provisions of the Money Laundering and Financial Crimes Strategy Act of 1998<sup>19</sup> and the 1998 State of New Jersey Working Group on Money Laundering<sup>20</sup> exemplified this importance. The DrugMARKET study was concluded after nine months and a final report was produced which documented its findings. This report offered twelve specific recommendations for new technology areas to assist in future investigations and project developments. The Project DrugMARKET report provides a logical springboard for analysis of the money laundering problem both from the prospective of technology and investigator needs, but also as it may be viewed by the forensic accountant or fraud examiner.

The specific research questions addressed by this research paper will be:

1. Do existing accounting rules and standards of practices have direct application and provide enough utility to auditors in the field of banking during the investigation of money laundering cases?
2. Do the twelve candidate technologies developed from the findings of the DrugMarket study team, provide utility to auditors, forensic accountants or Certified Fraud Examiners (CFEs) working such cases in the field of banking?

---

<sup>17</sup> HIDTAs are regions within the U.S. having critical drug trafficking problems that have a harmful impact in other areas of the U.S. HIDTAs task forces are made up of IRS and DEA agents as well as local and state law enforcement agencies.

<sup>18</sup> David Vaurio, "Project DrugMARKET Interim Final Report" 5., 7 November 1999, Arlington, VA.

<sup>19</sup> This Act added eight new provisions to the BSA, in order to assist state and local enforcement agencies and prosecutors in money laundering investigations and prosecutions.

3. Can any additional technologies be identified from an auditor, forensic accountant or CFEs professional perspective, which would be viewed as an asset to their work in money laundering cases in the field of banking?

### **Significance of the Study**

Increased use of information technology, coupled with the rapidly changing legislative and regulatory environments directed at interdicting and disrupting money laundering provide an opportune setting for scholarly research. This study took the basic conclusions derived from the DrugMARKET findings, made certain modifications and a change of focus to develop additional findings and make recommendations to those combating money laundering. Among the proposed outcomes will be an articulation of techniques, tools and procedures targeted against money laundering, as well as contributions to the professional body-of-knowledge for accountants which would help in "routine" audit work.

### **Objectives of the Study**

1. Emphasize that there is an urgent need for the review of internal controls at financial institutions with regards to money laundering and technology and make changes where necessary.
2. Underscore the urgency that auditors of financial institutions need to be trained better to understand their (the auditor's) functions and practical application when it comes to money laundering.

---

<sup>20</sup> In 1998, the New Jersey Governor directed the New Jersey Attorney General to convene a Working Group to review the current system of combating money laundering and to make

3. Define the important roles that management and other employees play in assisting auditors in monitoring and complying with internal controls.

### **Review of the Literature**

Numerous studies (at the federal, state and local law enforcement levels) have been conducted on the impact of money laundering and ways to detect and counter it using technology. However, those studies have focused on the law enforcement side of detection. Most studies, even those done by the Defense Advanced Research Projects Agency (DARPA)<sup>21</sup>, the DoD agency known for its ability to get things done using new technology, have shown that although law enforcement agencies have made dents in money laundering operations, it has been too little.<sup>22</sup> If not provided with greater assistance using greater technology, criminals will always be able to stay ahead of law enforcement.

It is wishful thinking to expect technology to resolve all of our problems, including money laundering. The modern financial system provides many more criminal opportunities than law enforcement can ever hope to forestall or block even with anti-laundering technology. New technological developments such as "smart cards" and "cyber-cash" will facilitate money laundering activities and provide new opportunities for money transfers that could be difficult if not impossible for government authorities to monitor or detect. Therefore, bank auditors become the *de facto* mainline of defense.

---

recommendations for improvement where appropriate.

<sup>21</sup> DARPA is the central research and development organization for DoD. It manages and directs selected basic and applied research and development projects for DoD, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions and dual-use applications.

<sup>22</sup> Law enforcement efforts recover only \$100 - \$500 million each year of the estimated \$300 - \$500 billion laundered.

It is hoped that the conclusions contained herein will influence the judgment of auditors and policy-makers within the fields of banking and law enforcement by convincing them that auditors/forensic accountants need additional assistance, not just with technology, but with training when it comes to money laundering. Due to the overwhelming amount of information available, the complexity of the topic, the number of methods/schemes used and the global financial system which we all operate within, this research paper is limited in scope to focus on auditors/forensic accountants in the United States banking industry.

### **Research Methodology**

This fact-finding research involved use of a structured-interview or questionnaire instrument, prior to interviewing practicing Forensic Accountants (FA), Certified Fraud Examiners (CFE),<sup>23</sup> or other related professionals. All prospective interviewees/respondents self-reported at least five years prior experience with money laundering cases. For the purposes of this study, the ideal operational definition of a forensic accountant was a practicing Certified Public Accountant (CPA) with the appropriate expertise and preferably holding designation with the American Board of Forensic Accountants. The ideal operational definition of a certified fraud examiner was a practicing CPA with the appropriate expertise, and holding designation with the Association of Certified Fraud Examiners. It must be noted, however, that not all

---

<sup>23</sup> Forensic accountants and CFEs are often retained by insurance companies, banks, police forces, government agencies and other organizations to analyze, interpret, summarize and present complex financial and business related issues in a manner which is both understandable and properly supported. They utilize accounting, auditing and investigative skills when conducting an investigation and often testify in court as expert witnesses.

respondent forensic accountants and certified fraud investigators are practicing CPAs. This type of respondent was chosen because individuals with these credentials are asked by both the banking industry and law enforcement to assist with money laundering investigations.

### **Sources**

This study derives original content from face-to-face, phone or questionnaire-structured interviews, as well as from scholarly writings and various federal and state governmental reports on money laundering. Additionally, more esoteric forensic accounting and fraud investigating practitioner literature offers an occasional article on strategies, techniques, and practice guidelines for approaching money laundering cases. Conclusions and recommendations will be derived from the evidence provided by the above-mentioned sources.

## CHAPTER 2

### INTERNAL CONTROL

#### **Background**

Auditing differs from accounting in that auditing involves investigation, verification, and evaluation, whereas accounting is the "bookkeeping methods involved in making a financial record of business transactions. . . ." <sup>24</sup> In other words, auditors, evaluate and verify the quality of control over financial matters that accounting methods and procedures maintain (i.e., the accounting control system).

Although the objectives and concepts that guide present-day audits were almost unknown in the early part of the twentieth century, audits of one type or another have been performed throughout recorded history. The original meaning of the word is "one who hears" and is appropriate to the era during which governmental accounting records were approved only after a public reading in which the accounts were read aloud. <sup>25</sup>

In today's environment, the auditor is considered the "eyes and ears of management." Auditing, however, was not recognized as a necessary function of modern times until the 1920s. Up until that time, auditors were employed by the owners of large-scale corporations to observe "management" and the day-to-day operations of the business. In other words, the absentee owner turned to auditors to protect the owner's interests from unintentional errors and fraud committed by managers and employees. Thus, audits often included a study of all, or almost all, transactions. Banks, as the primary institutional outside users of corporate financial reports also employ auditors,

---

<sup>24</sup> *The American Heritage Dictionary of the English Language*, Boston, MA 1981.

<sup>25</sup> Whittington, Ray and Pany, Kurt. *"Principles of Auditing*, 11<sup>th</sup> Ed. Chicago, IL. (1995): 7

because of concerns as to whether the financial reports provided by businesses were distorted by errors or fraud.

With the expanding U.S. economy, there were fears of inflated balance sheets and erroneous income statements. The banking industry began to require independent verification of company financial statements in order to approve loans. Thus, the field of auditing added new goals to determine whether financial statements provided a full and fair picture of financial position, operating results, and changes in financial position. As a result, fraud detection was no longer the single focus. This new emphasis was a "due diligence" response to the increasing number of shareholders and the corresponding growing number of corporate entities.

Partly as a consequence of the 1929 Crash, the Securities Act of 1933 and the Securities and Exchange Act of 1934 were born, in an attempt to protect the public from overeager and fraudulent businessmen. The purpose of the legislation was to regulate the securities and banking industries. The accounting profession was seen as the logical group through which to accomplish compliance with these new laws because accounting dealt with rules for the treatment of financial statements. A discipline for verification of these statements was also necessary, however, making the case for the need for auditors. Publicly traded companies needed independent accountants to verify the adequacy of financial statements; thus, fairness of reported earnings became of utmost importance.

These publicly traded companies also needed information about their own internal workings which an independent accountant could not provide because this was beyond the scope of independent verification. Therefore, companies hired internal auditors to assist the independent accountants with their verification of accounting records and also

to perform reviews of compliance with company policies and procedures and internal accounting controls.<sup>26</sup> Auditors found that by studying the internal controls, areas of strengths and weakness could be identified. Where internal controls were weak, auditors learned that they needed to expand the nature and extent of their tests.

As large corporate entities rapidly developed, auditors began sampling random transactions rather than studying all transactions. Since businesses exist to make profit, and auditing is a cost to the business, auditors and business managers quickly came to accept the proposition that careful examination of a few randomly selected transactions would be a cost-effective, and yet reasonably reliable indicator of the accuracy of other similar transactions.

With increased reliance upon sampling and internal control, professional standards began to emphasize limitations on the auditors' ability to detect fraud. The auditing profession recognized that audits designed to discover fraud would be too costly and therefore, good internal controls were considered far better fraud protection than audits. This belief faded in the late 1960s. During this time, large-scale fraud detection assumed a greater role in the audit process and the auditing profession began to use the term "irregularities" to describe fraudulent financial reporting and misappropriation of assets. This shift in emphasis resulted from increased congressional pressure that auditors assume more responsibility for large-scale frauds. There were several successful lawsuits claiming that management fraud had improperly gone undetected by

---

<sup>26</sup> Ibid. 24. Internal controls consist of policies, procedures or activities that serve to safeguard assets, maintain the accuracy of financial data, improve operational efficiency, and enforce adherence to management's policies.

independent auditors, which has led to an increasing acceptance by many public accountants that audits should be expected to detect material irregularities.

With the late 1980s and early 1990s, came the multi-billion dollar "bail out" of the savings and loan industry. Public outcry caused a movement towards increased regulation of federally insured financial institutions. Both Congress and regulatory agencies believed that the key to preventing similar problems was to enact effective laws and regulations such as the FDIC Improvement Act of 1991.<sup>27</sup> Due to increased pressure and calls for government regulation of the accounting industry, the AICPA co-sponsored the *National Commission of Fraudulent Financial Reporting* to study the causes of fraudulent reporting and make recommendations to reduce the number of incidents. The Commission's 1987 final report, made a number of recommendations for auditors, public companies, regulators and educators. Recommendations led to the development of an internal control framework used for evaluating the internal controls of organizations. The development of these internal control criteria increased the demand for attestation by auditors to the effectiveness of internal controls.

This movement toward increased auditing oversight and internal controls is concurrent to the recognition by regulators and others, that similar control mechanisms and processes might provide important safeguards to detect money laundering. With the financial services industry so vulnerable; studies, reports, and investigations recurrently document the need to remediate these vulnerabilities to money laundering transactions.

---

<sup>27</sup> The FDIC Improvement Act of 1991 required the management of large financial institutions to engage auditors to attest to management's assertion about the bank's compliance with laws and regulations related to safety and soundness of the institution.

When financial transactions were recorded and posted by hand and other accounting procedures that were used to complete the accounting cycle could be manually traced, auditors could visually observe the audit trail to determine their appropriateness. Today, however, since the introduction of computers, auditors cannot visually inspect posted transactions, not only because of sheer volume, but because all data and accounting procedures are "hidden"; stored within the computer in electronic format making observation of the accounting process difficult. The rapid growth in technology, most notably the development of electronic data processing (EDP), has greatly challenged auditors when monitoring the processing of accounting data and evaluating internal controls. The internal control procedures once established under both manual and mechanical systems have for the most part been compromised.

In order to assist auditors, the AICPA had developed ten generally accepted auditing standards (GAAS) which define objectives and provide guidance to auditors while conducting an audit. These standards are broken into three areas: General, Field Work, and Reporting Standards.

#### **General Standards (GS)**

1. The audit is to be performed by a person or persons having adequate technical training and proficiency as an auditor.
2. In all matters relating to the assignment, an independence in mental attitude is to be maintained by the auditor or auditors.
3. Due professional care is to be exercised in the performance of the audit and the preparation of the report.

#### **Standards of Field Work (FW)**

1. The work is to be adequately planned and assistants, if any, are to be properly supervised.

2. A sufficient understanding of the internal control structure is to be obtained to plan the audit and to determine the nature, timing, and extent of the tests to be performed.
3. Sufficient competent evidential matter is to be obtained through inspection, observation, inquiries, and confirmation to afford a reasonable basis for an opinion regarding the financial statements under audit.

### **Standards of Reporting (SR)**

1. The report shall state whether the financial statements are presented in accordance with generally accepted accounting principles.
2. The report shall identify those circumstances in which such principles have not been consistently observed in the current period in relation to the preceding period.
3. Informative disclosures in the financial statements are to be regarded as reasonably adequate unless otherwise stated in the report.
4. The report shall either contain an expression of opinion regarding the financial statements, taken as a whole, or an assertion to the effect that an opinion cannot be expressed. When an overall opinion cannot be expressed, the reasons therefor should be stated. In all cases where an auditor's name is associated with financial statements, the report should contain a clear-cut indication of the character of the auditor's work if any, and the degree of responsibility the auditor is taking.<sup>28</sup>

Of these standards, four (GS-1, FW-1, FW-2 and FW-3) have been severely affected by EDP systems, placing additional burdens upon auditors that were not encountered in manual or mechanical systems.

The first one is in the general standard that states "the audit is to be performed by a person or persons having adequate technical training and proficiency as an auditor."

---

<sup>28</sup> Whittington and Pany. 32-33.

In today's environment, this means that auditors not only have to be up-to-date with their knowledge on GAAS, generally accepted accounting practices (GAAP), and compliance regulations established by a number of federal agencies but they must also be familiar with sophisticated computer technology. Computers are no longer just tools for performing routine tasks quickly and without error. They can delete, change, and edit any transaction done in the past without leaving any paper trace or even electronic traces.

The second compromised GAAS is the standard of field work that states "the work is to be adequately planned and assistants, if any, are to be properly supervised."

In the planning of the overall strategy for the conduct and scope of an audit, the auditor is faced with the evaluation and testing of six additional accounting controls, four general controls and two application controls,<sup>29</sup> beyond those necessary for a manual or mechanical accounting system. In addition, "assistants . . . are to be properly supervised," demands more of the auditor attention in that the auditors must not only direct accounting tasks, but supervise and monitor these tasks on a complex computer systems which they already have difficulty understanding.

The third GAAS is the second standard of field work: ". . . sufficient understanding of the internal control structure is to be obtained to plan the audit and to determine the nature, timing, and extent of tests to be performed." To obtain a better understanding of what is meant here, specific requirements are set in the auditing interpretation on assessing control risk. The auditor must:

---

<sup>29</sup> General controls are defined as having pervasive effects, implying that if they are weak or absent, they may negate the effects of the application controls. The general controls are: 1) organization, personnel practices, and standard operating procedures, 2) systems development and documentation, 3) hardware and systems software, and 4) systems security. Application controls are defined as those relating to the specific tasks performed by the computer. The application controls are: 1) data capture and batch data entry and 2) on-line entry, processing, and output. Watne, Donald and Turney, Peter. *Auditing EDP Systems.*, 2<sup>nd</sup> Ed.(New Jersey: Englewood Cliffs, Prentice Hall, 1990), 119.

consider . . . the complexity and sophistication of the entry's operations and systems, including whether the method of controlling data processing is based on manual procedures independent of the computer or is highly dependent on computerized controls. As . . . operations and systems become more complex and sophisticated, it may be necessary to devote more attention to internal control structure elements to obtain the understanding . . . to design effective substantive tests.<sup>30</sup>

The last standard to be greatly affected by the use of EDP is the third standard of fieldwork. It requires "sufficient competent evidential matter to be obtained . . . " In an EDP system, both the type of evidence to be gathered and the means through which the evidence is collected has changed. Source documents no longer exist or are very difficult to obtain and verify. Information is stored in electronic format, replacing journals and ledgers. The auditor also must use various computer programs in place of visual examination of documents generated by the manual or mechanical systems.

It must be noted however, that the auditors are responsible only for the review and the expression of an opinion on the internal control system. They can recommend changes and improvements in internal control but it remains management's responsibility and judgement whether to implement those changes. Many auditors have a struggle with this disconnected responsibility because management will not always make recommended changes. For example, "Citigroup Inc. [Citibank] co-Chairman John Reed failed to take decisive action after internal bank warnings for several years . . . showed the bank was ignoring its own safeguards against money laundering. . . ." <sup>31</sup>

Management must adopt an internal control structure that will record, process, summarize and report financial data. This is not accomplished with the general ledger

---

<sup>30</sup> Statements of Auditing Standards (SAS) No. 55 (as revised by SAS No. 78).

<sup>31</sup> Day Kathleen, Washington Post "Probe Targets Citibank Safeguards", 5 November 1999: A10.

alone but with all other reporting systems that support the general ledger. Therefore, all computer programs that feed the general ledger are an integral part of the company's internal control structure. Furthermore, the data processing environment (operating system, on-line systems, database systems and the like) in which all these applications operate is also an integral part of the internal control structure. It is this internal control structure that supports the financial reports. The EDP auditor must evaluate the adequacy and effectiveness of this internal control structure.

### **Research Process**

For purposes of this study, the experience and insight of experts was sought for the purposes of identifying additional information applicable to the detection and monitoring of potential or actual money laundering in banking. A questionnaire was directed to interviewees with knowledge of financial crimes and money laundering, with the objective of deriving and capturing insights not acquired during Project DrugMARKET. It is assumed that the insights from these persons with specialized knowledge have considerable research value and can contribute to the professional body-of-knowledge.

### **Question #1**

Do existing accounting rules and standards of practices have direct application and provide enough utility to auditors in the field of banking during the investigation of money laundering cases?

## **Findings**

The respondents agreed with most of the literature on the subject of money laundering, one stating "it is difficult to label individual transfers of funds, persons, accounts, or businesses as definitely being associated with money laundering within the time frame relevant to crime detection".<sup>32</sup> Often, years elapse between the time that transfer records are generated and the conclusion of the investigation of relevant leads or suspects. It is known among law enforcement that they clearly cannot identify or prosecute all money laundering activities (See Figure 1 and 2)<sup>33</sup> and it is impossible for law enforcement to label with certainty each transfer of funds as licit or illicit by merely looking at any set of transfers. Figure 1 shows that only a fraction of cases worked result in a penalty, while Figure 2 shows the increasing amount of time to process a single case.

---

<sup>32</sup> Respondent No. 6: White Collar Crime Analyst, Phone Interview, 6 December 1999.

<sup>33</sup> The Financial Crimes Enforcement Network (FinCEN) is the information-development and analytical unit within the Department of Treasury, that supports law enforcement agencies with the analysis of Currency Transaction Reports (CTRs) in order to discover money laundering activities. In a General Accounting Office report to Congress, FinCEN was criticized that it "... Needs to Better Manage Bank Secrecy Act Civil Penalty Cases", 1998.

Figure 1

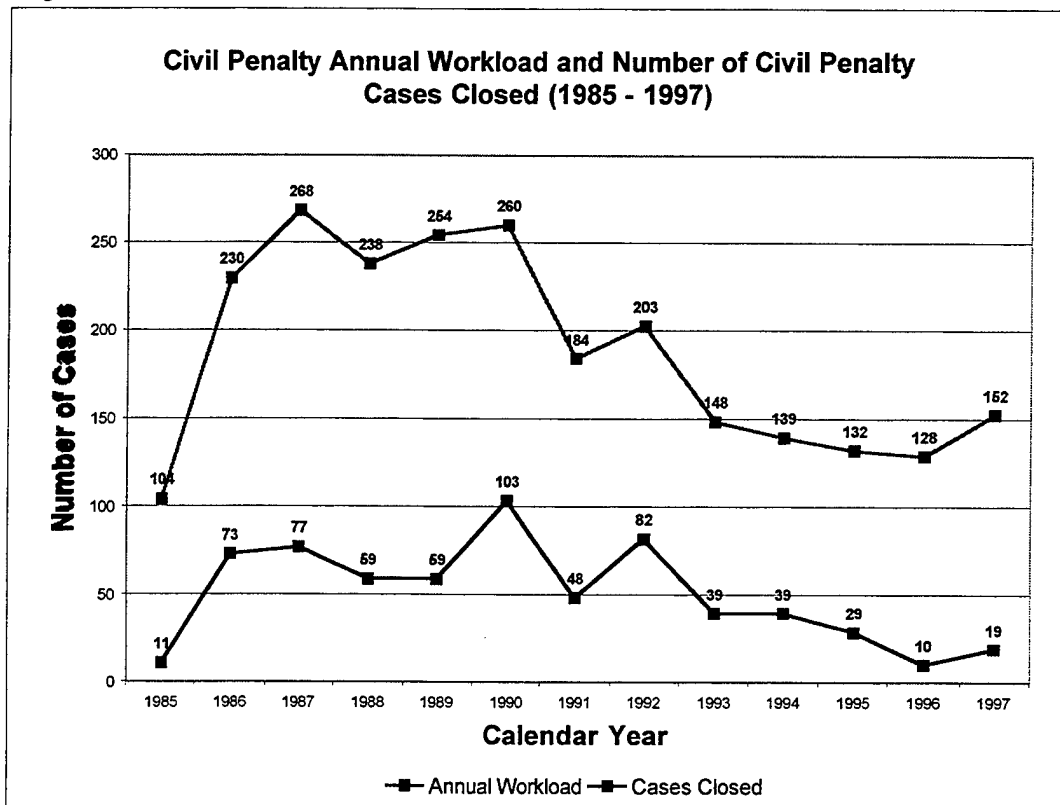
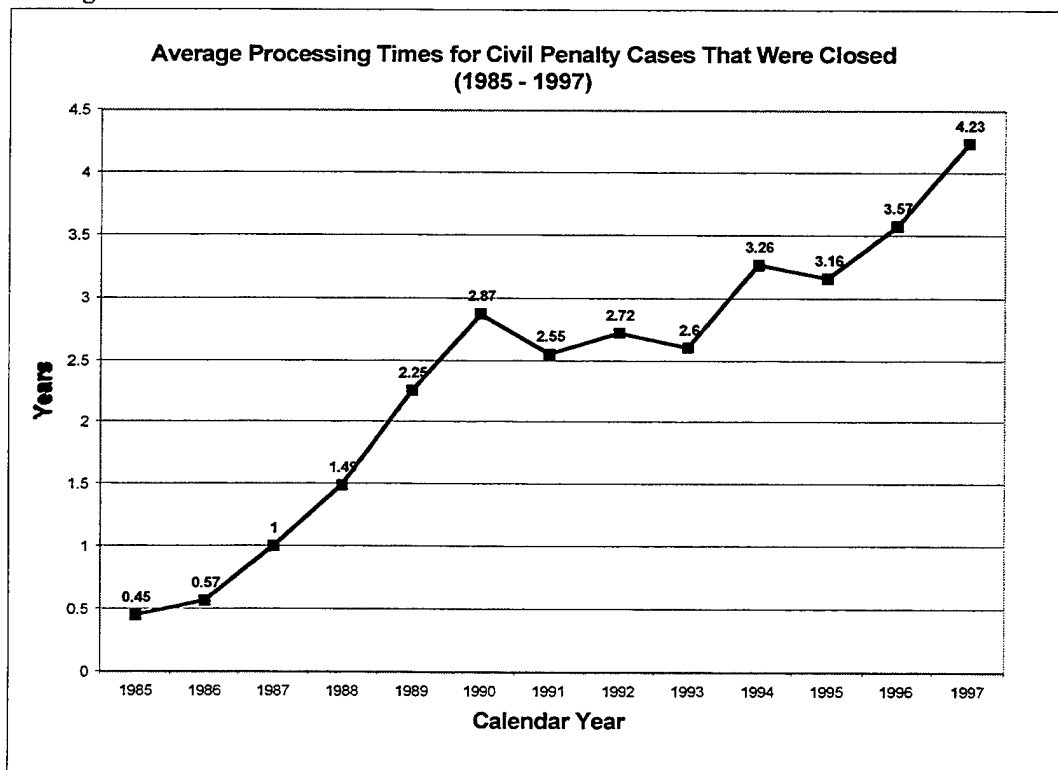


Figure 2



Thus, law enforcement can greatly benefit from the assistance of banking auditors to identify money laundering activities.<sup>34</sup> In order for auditors to assist law enforcement, the consensus was that banking auditors must tighten and monitor their internal controls more closely.

The consensus among the respondents also concluded that no one accounting or auditing standard specifically deals with the issues of money laundering. The respondent identified as the Principal Investigator/FACFE, however, stated that several years ago, four documents were issued as a result of continuing efforts to define, assess, report on, and improve auditing internal controls. These documents were issued by: the Institute of Internal Auditors Research Foundation's Systems Auditability and Control (SAC); the Committee of Sponsoring Organizations of the Treadway Commission's<sup>35</sup> Internal Control -Integrated Framework (COSO);<sup>36</sup> and the AICPA's Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (SAS

---

<sup>34</sup> Several respondents noted: "Banks are not law enforcement agencies. They are in the business for profits first and foremost." For this reason, it is widely believed that banks meet the very minimum of the "letter of the law" when it comes to money laundering surveillance, and not the "spirit of the law". Cost and/or loss of customers are the banks greatest concern. Banks for the most part cannot be blamed for this attitude because regulators are unwilling to impose harsh penalties (i.e. revoke a banks charter on the basis of BSA violations) for fear of hurting investors. U.S. Congress., 11.

<sup>35</sup> The Treadway Commission was a major U.S. study sponsored by Financial Executive Institute, American Institute of Certified Public Accountants, Institute of Internal Auditors and two other major organizations in response to the U.S. savings and loan crisis and the widening expectation gap. This report recommended that management of public companies formally acknowledge in annual reports responsibility for internal control related to financial reporting, discuss how they fulfilled their responsibilities, and provide their assessment of the effectiveness of internal controls. The public representation on the effectiveness of the company's internal controls by senior management was the most radical component of this recommendation. [http://www.kpmg.ca/crsa/crsa\\_int.htm#Treadway](http://www.kpmg.ca/crsa/crsa_int.htm#Treadway)

<sup>36</sup> This report, which was in response to the Treadway Report recommendations, proposes a five-category control framework which organizations and regulators can use to assess control effectiveness. The COSO report calls for chief executives to initiate a self-assessment of their control system but avoids comment on the issue of mandatory reporting on internal control. [http://www.kpmg.ca/crsa/crsa\\_int.htm#COSC](http://www.kpmg.ca/crsa/crsa_int.htm#COSC)

78).<sup>37</sup> Because each of the issuing bodies are different and developed the documents to address the specific needs of their own audiences, some disparities do exist. The intended audiences, i.e., internal auditors, management, and external auditors, all devote much time and effort toward establishing or evaluating internal controls (See Table 3).

#### SAC Report

The SAC report defines the system of internal control, describes its components, provides several classifications of controls, describes control objectives and risks, and defines the internal auditor's role. The report provides guidance on using, managing, and protecting information technology resources and discusses the effects of end-user computing, telecommunications, and emerging technologies.

#### COSO Report

The COSO report defines internal control, describes its components, and provides criteria against which control systems can be evaluated. The report offers guidance for public reporting on internal control and provides materials that management, auditors, and others can use to evaluate an internal control system. Two major goals of the report are to (1) establish a common definition of internal control that serves many different parties, and (2) provide a standard against which organizations can assess their control systems and determine how to improve them.

#### SASs 55 and 78: Statements on Auditing Standards

SASs 55 and 78 define internal control, describe its components, and provide guidance on the impact of controls when planning and performing financial statement audits.<sup>38</sup>

---

<sup>37</sup> SAC (1991, revised 1994) offers assistance to internal auditors on the control and audit of information systems and technology. COSO (1992) makes recommendations to management on how to evaluate, report, and improve control systems. SASs 55 (1988b) and 78 (1995) provide guidance to external auditors regarding the impact of internal control on planning and performing an audit of an organization's financial statements.

<sup>38</sup> Colbert, Janet and Bowen, Paul, Book Review: *A Comparison of Internal Controls: CobiT, SAC, COSO and SAS55/78*, Information Systems Audit and Control Association, 1999. [http://www.isaca.org/bkr\\_cbt3.htm](http://www.isaca.org/bkr_cbt3.htm)

**Table 1**

Comparison of Internal Control (IC) Concepts	SAC	COSO	SASs 55/78
Primary Audience	Internal Auditors	Management	External Auditors
IC viewed as a	Set of processes, subsystems, and people	Process	Process
IC Objectives	Effective & efficient operations, Reliable financial reporting, Compliance with laws & regulations	Effective & efficient operations, Reliable financial reporting, Compliance with laws & regulations	Effective & efficient operations, Reliable financial reporting, Compliance with laws & regulations
Components	Control Environment Manual & Automated Systems Control Procedures	Control Environment Risk Management Control Activities Information & Communication Monitoring	Control Environment Risk Assessment Control Activities Information & Communication Monitoring
Focus	Information Technology	Overall Entity	Financial Statements
IC Effectiveness Evaluated	For a period of time	At a point in time	For a period of time
Responsibility for IC System	Management	Management	Management

The Principal Investigator/FACFE believed that these reports, if followed, would be of some help to auditors in the banking industry. He noted however, as did others, "that no matter how well an internal control system is designed and operated, it can only provide a reasonable assurance regarding achievement of an entity's objectives".

### **Implications and Recommendations**

Auditors in the banking industry must review internal control procedures, training programs and other processes in an attempt to ensure that they are making proper "due diligence" and a "good faith" effort to detect money laundering. They must also follow established standards set by the AICPA and other accounting/auditing authorities while conducting their audit. It is recommended that auditors read the four reports that are mentioned above, SAC, COSO, SAS 55 and 78, as these reports will assist auditors in evaluating the internal controls of their organization.

In today's environment, even the tightening of internal controls within the banking industry will not be enough, to sufficiently disrupt the flow of illegal funds. This fight requires that the banking industry receive advanced technology in order to assist and remove some of the burden from auditors. Both the banking industry and law enforcement community would greatly benefit from better technology. Banks would be able to provide "higher quality" reports on suspicious activity, thus reducing their costs of processing reports, and reducing the number of reports the Financial Crimes Enforcement Network (FinCEN) receives on a daily basis.<sup>39</sup>

---

<sup>39</sup> The American Bankers Association, estimates that the average mid-size bank spends \$3-5 per report filed. FinCEN receives an average of 30,000 CTRs every day. If the quality of reports increase as the volume of reports decrease, then maybe more cases could be completed. General Accounting Office. 3.

## CHAPTER 3

### TECHNOLOGY

#### **Background**

Law enforcement officials describe money laundering as a three-step process, beginning with the placement of currency into a financial services institution ("placement"), transferring it into and then out of several bank accounts, or exchanging it for travelers' checks or a cashier's check, so as to confuse the audit trail. They then hide the source and ownership of funds ("layering"), and conclude with the reinvestment of those funds in an seemingly legitimate business thus providing a plausible explanation for its ownership ("integration").<sup>40</sup>

While countermeasures to all three components of money laundering are important, laundered money is most vulnerable, and the probability of detection greatest, at the placement stage. It is at this stage that "smurfs" would have to go into banks and "structure" deposits so as to be under the \$10,000 reporting requirement. In the layering stage, efforts are made to ensure that illicit funds are difficult to differentiate from licit funds. This is done by exploiting the "frequency, volume and complexity" of bank-to-bank transfers.<sup>41</sup> This ensures that illicit money is impossible to differentiate from money obtained through legitimate means and so integration can be achieved. This framework is useful for understanding the dynamics of many money laundering schemes. It should be

---

<sup>40</sup> Winer, 2.

<sup>41</sup> It is extremely difficult to find wire transfer records after the fact, in order to reconstruct the flow of money, unless the name or account number, the time and place of origin, or other specific characteristics are known. In addition, either a search warrant or a subpoena is generally required for law enforcement agents to view domestic wire transfer records in electronic form.

noted however, that in many cases, illicit funds have been both layered and integrated as licit proceeds of legitimate business (i.e., cash-based businesses such as restaurants and casinos) before they go into the financial system. For this reason, money laundering detection is extremely challenging for law enforcement since it does not always follow this three step process or any other set pattern. As a possible way out of this impasse, it has been proposed by several law enforcement agencies that greater use of advanced technology be used to assist law enforcement in recognizing and flagging unusual activities or recurring suspicious patterns in fund transfers.<sup>42</sup>

At the strategic level, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has long-recognized the need to accelerate its technological innovations in an attempt to deter and counter money laundering. The agency's current Strategic Plan emphatically identifies technology as one of the critical factors that must be enhanced for success. The Strategy articulates this intent by stating:

FinCEN's strength rests in its ability to rapidly adapt to the constantly changing world of money laundering through the application of state-of-the-art technology, and its efforts to analyze data, identify trends and patterns, and develop anti-money laundering programs both domestically and internationally.<sup>43</sup>

FinCEN has had successes as well as difficulties in its technological innovations and systems over the past decade.<sup>44</sup> In its current Strategic Plan, FinCEN proposes three strategies and six accompanying performance measures of effectiveness in its stated

---

<sup>42</sup> Several federal law enforcement agencies are involved in control of money laundering. They include, within the Department of Justice, the Federal Bureau of Investigations (FBI) and the Drug Enforcement Administration (DEA); and, within the Department of the Treasury, the Internal Revenue Service (IRS) and the U.S. Customs Service.

<sup>43</sup> U.S. Department of Treasury, *Financial Crimes Enforcement Network, 1997-2002 Strategic Plan*, 1997, 35.

<sup>44</sup> David Vaurio, phone interview by author, 10 November 1999.

effort to incorporate and upgrade to state-of-the-art technologies.<sup>45</sup> The prospects for success on these initiatives remains uncertain and there is a lack of consensus among experts whether FinCEN's strategy and capital investments are necessarily the "cure all" it is purported to represent.<sup>46</sup>

Several other governmental agencies have inserted themselves in the technology front. In the past, DARPA funded basic algorithm research to be used in money laundering detection,<sup>47</sup> and the Office of National Drug Control Policy (ONDCP) distributed demonstration software that has been found to be of limited utility by potential enforcement users.<sup>48</sup>

At the operational level, some of the innovative thinking and case demonstrations in money laundering investigations and prosecutions have originated from the Phoenix Financial Task Force. The Arizona Attorney General has hosted the Southwest Border Money Laundering Conference on Money Laundering Enforcement and Computer Technologies for the past seven years. The 1998 and 1999 Conference proceedings provide most of the current problem statements and requirements definitions from real-world practitioners.

---

<sup>45</sup> U.S. Department of Treasury, 22.

<sup>46</sup> David Vaurio, "Project DrugMARKET Interim Final Report" 5., 9.

<sup>47</sup> DARPA's interest in money laundering was primarily related to terrorism and the illegal sale of arms rather than drug trafficking. The agency funded several projects to explore the feasibility of using artificial intelligence techniques to detect electronic money laundering, but when the budget was tightened in 1992, these projects were dropped. Dr. Edward Carapezza, DARPA Program Manager, Advanced Technology Office, interview by author, 11 December 1999.

<sup>48</sup> The ONDCP in the Executive Office of the President attempts to develop overall policy directions for drug control and control of drug-related money laundering. The demonstration software that it provided to law enforcement, did not have the capability to run actual test data, and the capabilities of the software was questionable since it was both undocumented and unsupported. David Vaurio, phone interview by author, 10 November 1999.

The Task Force is in the vanguard for organizational structure and technological applications, as it fulfills Arizona's legislative initiatives to counter money laundering.

- 1) Arizona has been one of the first and most active civil racketeering (RICO) prosecution units in the country since 1980.
- 2) Arizona requires businesses that have special strategic significance to law enforcement to maintain records of cash transactions and of transactions that are otherwise suspicious.
- 3) Arizona regulates businesses that are especially vulnerable to money laundering pressures.<sup>49</sup>

The Attorney General's Financial Remedies Unit (FRU) and Transaction Records Analysis Center are models of technological applications and creative practices and procedures, including banking surveillance and money laundering detection. It was the FRUs innovative practices and practitioner requirements that led to a call for new prospects technological solutions to counter money laundering.

Technology maybe the "cure" to countering the scope, magnitude, and speed of money laundering, but it is also the "cause". As technology continues to expand in the banking industry through the use of a global financial system, allowing for multiple points of entry and extremely rapid transmission of funds, it continues to hamper efforts of law enforcement.

New banking practices that provide customers with on-line 24-hour banking capabilities and new forms of electronic money (i.e., smart cards, cyber-cash, and e-payments), make banks a very desirable place to hide illegal funds. It is projected that by

---

<sup>49</sup> Beckman, Dr. Robert, *"The Phoenix Financial Task Force, Southwest Border HIDTA"* (Arlington, VA: 1999) 3, 5.

the end of 2000, over 25 million Americans will be using e-purchase capabilities on a regular basis,<sup>50</sup> and e-commerce could increase to as much as \$3 trillion annually.<sup>51</sup>

These situations have caused many in the law enforcement community to believe that a more effective way to fight money laundering is to make all financial transactions more visible; (i.e., who, what, where, when, and how much, would be available for review by law enforcement when needed). This however will not be easy. Banks and other financial institutions continue to make greater strides to making extended use of anonymous digital cash so as to keep financial activities private. There is considerable resistance by private organizations to any efforts by law enforcement at establishing closer regulation of "cyber-transactions" from those who believe that the citizen's right to privacy outweighs the government's right to monitor such activities.

Conflicting theories of public policy are playing out in this issue. Libertarian perceptions contend that the state should do the "greatest good for the greatest number", which extrapolated, leads to a case for extraordinary powers for government if the intent is a public good. Constitutional scholars debate the limits of the power of the state with regard to "search and seizure" and "rights to privacy". Rulings by the U.S. Supreme Court are constantly defining case law and establishing precedent on this careful balancing of the rights of the individual verses the intrusion of state powers.

There is a great deal of argument, not only in legal circles, but also among various advocacy groups, concerning the intrusiveness of the state into the cyberworld. Many purport that the Internet should be a free, unfettered, and unbound domain. This proposition collides with the long established Constitutional power of the state to regulate

---

<sup>50</sup> WTOP News 107.7 FM, *Market Watch*, (November 1999)

<sup>51</sup> Winer, 24.

interstate commerce. Matters of scrutiny, integrity, and safety of an automated financial system remain a state interest. Suffice it to say, the privacy issue is a high visibility issue in which the policy, regulation, and Constitutional issues remain unsettled.

In addition to the areas of privacy, banks in the United States engage in a very active and complex web of bank-to-bank transfers, chiefly using two wire systems to carry out all exchanges. These systems are the Federal Reserve's electronic funds and securities transfer service (Fedwire), operated by the Federal Reserve Banks; and CHIPS (Clearing House for Interbank Payments System), operated by the New York Clearing House, an association of money center banks.<sup>52</sup> There are only about 15 or 20 banks in the United States that are categorized as "money center" or world-class banks, and operate globally. Most international wire transfers moving to and from the United States pass through one of New York City's large money center banks in order to access CHIPS. In a recent investigation by the Federal Bureau of Investigation (FBI), over the last three years nearly \$7.5 billion in laundered funds originating from Russia flowed through nine Bank of New York accounts.<sup>53</sup> According to recently published reports, the nine accounts at Bank of New York averaged \$6 million daily in deposits. In its defense, the Bank of New York stated that it "cannot be expected to perform an in-depth investigation of every unusual financial transaction by their customers," since on an average business day, about

---

<sup>52</sup> Approximately 9,500 banks have access to Fedwire; 115 large banks have direct access to CHIPS, some of which also act as intermediaries for middle-size and smaller banks. Approximately 150 U.S. banks and 300 U.S. based subsidiaries of foreign banks are users of SWIFT (Society for Worldwide Interbank Financial Telecommunication), an international messaging system that carries instructions for wire transfers between pairs of correspondent banks. In order to demonstrate how large the problem is, in 1998, some 98.4 Million (M) funds transfers with a total value of \$329 Trillion (T) were made over Fedwire -- an average of \$3.3M per transaction. About 38M transfers, worth \$207T, were originated by banks in the Second Federal Reserve District alone, which is served by the New York Fed. Another 15.4M Treasury and agency securities transfers, valued at \$205T, were processed over Fedwire. Of these, the New York Fed accounted for 11.5M transfers valued at \$162T.  
<http://www.ny.frb.org/pihome/fedpoint/fed43.html>

96,000 transactions (totaling nearly \$600 billion) pass through the wire room from its various businesses.

A serious problem for anti-money laundering objectives that law enforcement faces is with America's current laws on tracking wire transfers. The Electronic Communications Privacy Act forbids access by law enforcement personnel to electronic Fedwire and CHIPS records without a search warrant, or, for records stored for more than 180 days without a subpoena. Even with a search warrant or subpoena, it is generally necessary to provide to the Federal Reserve Bank all of the information needed to identify the specific targeted transaction.

With difficulties such as these facing law enforcement's efforts at combating money laundering, Project DrugMARKET was originated in order to explore any new technologies that may be able to assist law enforcement, if not to bridge the gap but to at least shorten it. The Project team kept a close relationship with the Arizona technology experts and conducted a baseline assessment of how the FRU evolved and operated under the auspices of the regional HIDTA. The Project concluded its efforts in a final report which documents its findings and contains twelve specific recommendations for new technological areas to explore in future investigations and project developments.

### **Research Process**

The twelve technologies, described more fully in Appendix A, were the result of a study known as Project DrugMARKET which was to baseline the state-of-the-art in money laundering investigation capabilities of the field investigator and the prosecutor.

---

<sup>53</sup> Seltzer, Mark., *Fighting Money Laundering*, Boston Globe, 2 November 1999, C04.

The objective was to discover what works and what does not, and how investigations could be conducted better, faster, and cheaper. These technologies constitute the basis for the second structured interview question directed to the expert respondents in this report.

## Question #2

Do the 12 candidate technologies (see attached) developed from the findings of the DrugMarket study team, provide utility to auditors, forensic accountants or Certified Fraud Examiners (CFEs) working money laundering cases in the field of banking?

Rank order (a minimum of 3) on the basis of their utility to the investigation/prosecution of money laundering cases and then rank order (a minimum of 3, unless you feel that none of these apply) on the basis of their utility to forensic accountants/ auditors working such cases. Comment on the top 3 technologies (also if none apply) for auditors/forensic accountants.

	Investigators/ Prosecutors	Auditors/ Forensic Accountants
1. Banking Industry SAR Algorithm	-----	-----
2. Case Reconstruction Demonstration Project	-----	-----
3. Cash Currency Processor	-----	-----
4. Currency Detection Study	-----	-----
5. Currency Serial Number Tracking	-----	-----
6. Digital Bank Subpoena Processor	-----	-----
7. El Dorado Docex Project	-----	-----
8. Electronic Money Laundering Case Template	-----	-----
9. Money Laundering Data Analysis & Visualization	-----	-----
Operational Test and Evaluation		

10. Paper Check Imaging Processor	-----		-----
11. Precision Query - Very Large Data Bases	-----		-----
12. Targeting Random Phone Use	-----		-----

Comments:

The responses and outcomes of these questions provide the content for the subsequent findings, and consequent implications and recommendations that follow in this chapter.

### **Findings**

Several respondents state that auditors differ from investigators in that the auditor's goal is to protect the depositor's and the shareholder of their bank, whereas, the investigator's goal is to assist in the prosecution of criminal activity and thereby reducing crime. With this in mind, the results of the different respondents is interesting.

The respondents were asked to rank order with what they believed were the top three projects from the DrugMARKET findings, with regards to utility to the investigation/prosecution of money laundering cases, as well as forensic accountants/ auditors working such cases, with regards to the banking industry. Comments also followed. Of the twelve projects that were reviewed, the majority of respondents clearly chose the Banking Industry SAR Algorithm Project and the Digital Bank Subpoena Processor Project, as being the most useful to both investigators and bank auditors. As opposed to the Projects chosen by the DrugMARKET findings (as noted by \*)

**Table 2:**

Technologies to Assist Law Enforcement	Proj. DM	Scoring				Respondents					
		Pts.	Ave.	% of Resp.	Score	#1	#2	#3	#4	#5	#6
1. Banking Industry SAR Algorithm		14	2.33	83%	1.94	2	1	1	1	1	
2. Case Reconstruction Demonstration Project		0	0.00	0%	0.00						
3. Cash Currency Processor	*	4	0.67	33%	0.22	1			3		
4. Currency Detection Study		1	0.17	17%	0.03	3					
5. Currency Serial Number Tracking		2	0.33	17%	0.06					2	
6. Digital Bank Subpoena Processor		8	1.33	67%	0.89		2		2	3	1
7. Document Exploitation Docex Project	*	0	0.00	0%	0.00						
8. Electronic Money Laundering Case Template		2	0.33	17%	0.06						2
9. Money Laundering Data Analysis		2	0.33	33%	0.11		3				3
10. Paper Check Imaging Processor		0	0.00	0%	0.00						
11. Precision Query - Very Large Data Bases	*	0	0.00	0%	0.00						
12. Targeting Random Phone Use		0	0.00	0%	0.00						

**Table 3:**

Technologies to Assist Bank Auditors	Proj. DM	Scoring				Respondents					
		Pts.	Ave.	% of Resp.	Score	#1	#2	#3	#4	#5	#6
1. Banking Industry SAR Algorithm		12	2.00	67%	8.00		1	1	1	1	
2. Case Reconstruction Demonstration Project		0	0.00	0%	0.00						
3. Cash Currency Processor	*	1	0.17	17%	0.17				3		
4. Currency Detection Study		0	0.00	0%	0.00						
5. Currency Serial Number Tracking		2	0.33	17%	0.33					2	
6. Digital Bank Subpoena Processor		8	1.33	67%	5.33		2		2	3	1
7. Document Exploitation Docex Project	*	5	0.83	33%	1.67	1					2
8. Electronic Money Laundering Case Template		0	0.00	0%	0.00						
9. Money Laundering Data Analysis		3	0.50	50%	1.50	3	3				3
10. Paper Check Imaging Processor		0	0.00	0%	0.00						
11. Precision Query - Very Large Data Bases	*	2	0.33	17%	0.33	2					
12. Targeting Random Phone Use		0	0.00	0%	0.00						

### Measurement of Effect:

Respondents ranked ordered their top three choices of the twelve DrugMARKET projects. In order to be fair in evaluating the results, each number was assigned a value. A score of: 1 = 3 points; 2 = 2 points; and 3 = 1 point. These numbers were added together to give each project its total value. Next, each project total was averaged, by dividing by the total number of respondents. Next, the percentage of respondents that chose a particular project was calculated. This percentage was then multiplied to the project average, which resulted in the project score. Example: See Table 3: Project No. 1: Four respondents chose this project and assigned it a "1" value, which equals a value of twelve (12). Next the average was calculated by dividing the value "12" by the six of

respondents, for a value of two (2). The percentage (67%) was calculated by dividing the four (4) respondents that chose this project by the total number of respondents (6). Multiplying the percentage by the average resulted in each project's overall score (8). This scoring system was to provide a method to account for the ranking each respondent gave each project as well as the number of respondents that chose that project.

### **The Banking Industry SAR Algorithm Project**

The majority of the respondents identified this project as number one on their list of importance with regards to investigators, stating that the law enforcement community does place a high importance priority on Suspicious Activity Report (SAR). Since this project suggests the requirement to increase the number of reportable SARs, in particular those SARs relating to money laundering, it would be far better to reduce the number of SARs at the same time as increasing the quality provided to law enforcement for further analysis and investigation. Several respondents also stated that because of the complexity of money laundering activities, and law enforcements lack of funds, investigators and "super" computers, the reporting of suspicious activities should be further limited as to concentrate searches to highly probable "suspicious" banks and known suspects, their immediate family and known contacts. Since law enforcement has only limited resources as compared to the number of organizations actually laundering money, it would be better to concentrate resources on shutting down or severely damaging a few organizations at a time rather than trying to merely annoy them all without significant success.

The majority of respondents also choose this project as the most significant, stating that improvements are needed in the banking industry's scanning reporting

abilities. It has been stated that law enforcement still has a hard time to discover new money laundering activities and they are the "experts". Therefore, auditors cannot be expected to discover anomalies without assistance. The banking industry would greatly benefit from such a system in which all transactions could be examined by computers using sophisticated algorithms and then followed-up by bank auditors before reporting to FinCEN. The Forensic Accountant/CFE feels that "banks do not want to follow-up on . . . [SARs]. Banks see their role as one of providing suspicious information to law enforcement agencies and leaving the follow-up tasks to law enforcement agents." The Principal Investigator/FACFE stated that "if banks are seen as complicit, bankers may be jailed and/or fined monetary penalties if convicted." It is suggested that at this point the "know-your-customer"<sup>54</sup> rules would apply, in order to make a better determination of the situation or questionable activity.

Lastly, the respondents stated that if such an automated system could be designed and deployed effectively, they did not believe such a system could, in-fact, track transactions in real-time as the Banking SAR Algorithm Project suggests; near real-time, but not real-time.

### **The Digital Bank Subpoena Processor Project**

The majority of the respondents also choose the Digital Bank Subpoena Processor Project as the second most important for investigators to obtain necessary documents (SARs, CTRs, etc.) in electronic format. The reason was that depending on the

---

<sup>54</sup> This new regulation would have greatly expanded the development of customer profiles by making bank tellers ask their customers where they got their money and what they planned to do with it. The FDIC received over 250,000 comments, almost all opposing the regulation. Congress, last year killed the resolution that would have made this law.

complexity of the information requested a bank's response time could be anywhere from days to months, leaving the trail cold. The form that the data ultimately arrives in is the core of the problem. The data provided are usually photocopies of original documents or of documents that were already transferred to microfiche. Thus, it is not uncommon for a bank to respond to a subpoena with several dozen large boxes filled with individual pieces of paper. In order for the underlying investigative value of each piece of paper to be determined, an analyst must physically look at each piece and "process" them in some manner, usually recording that information in either a ledger, electronic database or spreadsheet. This is a very time consuming process which is almost never completed due to the volume of paper and the shortage of analysts assisting investigators. What is ironic and frustrating to investigators is that most, if not all, of the data that were provided, was at some point in electronic format within the bank. If banks provided the requested information in electronic format, then investigators could both receive and process data quickly and more efficiently, and thus investigate more cases.

Again, the majority of the respondents felt that the project that would assist investigators most would also assist auditors the most. The reason is that if auditors could take the information requested by law enforcement and verify that it is correct on their "new" Banking SAR Algorithm system, this would ensure that the banks were providing "high quality" data to law enforcement. This could also be used as a training tool for auditors to identify suspected unlawful activities. Normally, some lonely clerk is making hundreds or thousands of photocopies (as stated above) while the auditor continues to make the same mistakes time-in and time-out.

## **Issues**

Respondents concurred that the greatest issue with either of these projects, as well as any other, is the cost to banks of implementation. Banks are in a profit making business and all regulatory requirements are addressed to the extent required, but least-cost to the institution. Generating, CTRs, SARs, etc., already imposes costs on banks. Tracking money laundering activities is a money losing activity for them. It is unrealistic to believe that banks would voluntarily implement a project that would add costs to their bottom-line and possibly lose prospective clients. Banks make money with funds that it holds for even 24-hours and would have little incentive for giving them up. Several respondents stated that if banks could turn these areas of loss into "profit", there stands a much better chance that banks would be willing to implement systems such as those proposed. If banks were given an incentive to look for money laundering activities, such as a percentage of all funds seized under asset forfeiture laws, they would be more willing to assist law enforcement rather than provide the minimum required.

## **Project DrugMARKET's Recommendations**

While several respondents in both categories of investigators and auditors chose the same projects that were recommended, there was no overwhelming attraction to these projects (Cash Currency Processor, Documentation Exploitation and Precision Query - Very large Data Bases) by those responding to this study. In fact, two of the projects - Documentation Exploitation and Precision Query - Very large Data Bases, were not even chosen under the heading of assisting law enforcement. The consensus among respondents was that there was no consensus. While the Forensic Accountant/CFE saw

currency detection as the weakest link in the evidence gathering process and as a result rated the Cash Currency Processors as a number one, others perceived it as having only limited value in that it assists only one or two agencies at most (i.e., Customs). Two respondents chose the Documentation Exploitation and Precision Query - Very large Data Bases Projects as items that would assist auditors by providing them with tools to analyze and obtain information and significantly reduce analytical time. The remaining respondents felt that these would have little value to auditors. The State Official/CFE went so far as to say that the Precision Query - Very large Data Bases Project was an impossible task to accomplish.

### **Implications and Recommendations**

Both the Banking Industry SAR Algorithm Project and the Digital Bank Subpoena Processor Project appear to have more perceived utility to both investigators and auditors than do the projects as recommended by the findings of Project DrugMARKET. While this study used a much smaller sample to obtain its findings, participants were a highly qualified group. This study did examine areas of both wire transfers and cyber-laundering, something that Project DrugMARKET did not do.

As in the case of Project DrugMARKET, if the problem domain of “money laundering investigations” remains high on the priority of national interests, then this report and the two technologies identified therein could serve as the foundation for a more focused community review and assessment of money laundering infrastructure support technologies. Such a review could be coordinated more appropriately by either the ONDCP and/or the National Institute of Justice.

## **CHAPTER 4**

### **EXPERT SYSTEMS**

#### **Background**

Research studies, government reports and Project DrugMARKET have all documented the importance of advanced expert systems in the discovery of money laundering activities. These findings have apparent value to the field of auditing. What follows are the highlights of key considerations regarding money laundering.

Knowledge-based systems, often called "expert systems" are technologies that rely upon techniques developed in the field of artificial intelligence (AI). They are essentially computer programs that emulate human thinking processes in problem-solving situations. The goal of an expert system is to arrive at the same result that a specific human mental process would produce.

Expert systems contain the following four components: knowledge base, inference engine, user interface and explanation facility. The knowledge base consists of facts in a specific topic area, and rules for using these facts. The rules are usually presented in the form of "if...then" statements. Many of the rules are really "rules of thumb" developed by the human expert (or group of experts) from their experience in the area. These rules are called heuristics and are "extracted" from the expert by knowledge engineers who place them into the knowledge base. The inference engine is a computer program that uses the information in the knowledge base. It drives the system by drawing an inference from related user-supplied facts to a knowledge base rule and then proceeding to the next fact and rule combination. This process forms a chain in which

the "then" part of one rule forms a link to the "if" part of the next rule, eventually reaching a conclusion. The user interface is the bridge between the inference engine and the user. It provides a communication facility between the two. Finally, the explanation facility helps the user understand why certain conclusions were reached. Thus, they are often designed so that they can display the path of evidence and facts used to reach a particular conclusion.

Expert systems differ from traditional decision support systems (DSS) in that the latter mainly uses computation in algorithms (step-by-step formulas) while the former relies on rules of thumb and the "gut instincts" of the expert.

Many benefits can be derived from the implementation of expert systems. They include:

- 1) Efficiency: Expert systems can significantly reduce the employee time required to plan and carry out an audit.
- 2) Distribution of Expertise: Since human experts are in short supply, expert systems provide the means of using knowledge in a wide number of locations without actually having the human expert on the premises.
- 3) Quality Control: Expert systems encourage consistent and uniform performance of professional tasks. Not only can expert systems provide guidance for various tasks, they can also help ensure that the key questions in performing a procedure have been addressed. This ensures quality control.
- 4) Education and Training: A significant investment of time and money is spent on the training of an auditor. Expert systems that provide professional recommendations against which developing auditors could test their judgments and sharpen their skills, would significantly reduce the investment that needs be made.<sup>55</sup>

---

<sup>55</sup> Brown, Carol and O'Leary, Daniel., *Introduction to Artificial Intelligence and Expert Systems*, 1995. [http://www.bus.orst.edu/faculty/brownc/es\\_tutor/es\\_tutor.htm](http://www.bus.orst.edu/faculty/brownc/es_tutor/es_tutor.htm)

Many expert systems are in existence today within both law enforcement and banking communities. FinCEN developed and uses a Financial Artificial Intelligence System (FAIS) to target suspicious patterns in all reports received under the BSA.<sup>56</sup> The IRS Detroit Computer Center and the U.S. Customs Service Data Center collect and store BSA reports that FAIS adds value too by evaluating and linking them to display possible patterns of suspicious financial activity. The FAIS uses three basic types of data for detecting money laundering: BSA transactions, subjects, and accounts. BSA's that can be associated with the same persons or business are then used to create the subject data element. BSA's that can be associated with the same bank accounts are used to create the account element. The grouping of BSAs into subjects and accounts is accomplished by examining information in the transactions (e.g., name, address, social security number). If these items are sufficiently similar, then two transactions are assumed to belong to the same subject. This data is then further analyzed by yet another expert system and sub-system of FAIS. This sub-system was derived from a system originally developed at the U.S. Customs Service for screening CTRs and was know as the Customs Artificial Intelligence System (CAIS). It was reengineered to function with FinCEN's system and is regularly updated to reflect changes in money laundering methods. These systems combined are used to evaluate the suspiciousness of the data. Based on indicators that appear directly within BSAs, and on additional indicators calculated from those BSAs, FAIS assigns a numeric suspiciousness score to each piece of data. On the basis of these

---

<sup>56</sup> More than 90 percent of these reports are CTRs.

scores and several other criteria, FinCEN analysts select subjects and accounts for further investigation using the link analysis component of FAIS. Link analysis is used to identify networks of financial activities that help to distinguish between legitimate business activities and money laundering.<sup>57</sup>

Many large bank's also use a set of relatively simple expert systems to screen transactions for illicit conduct. Some of these systems screen currency transactions to identify those which indicate "structuring", (e.g., five deposits of \$3,000 each in a single day). While other banks systems monitor wire transfers to look for countries or individuals that appear on a list compiled by Treasury's Office of Foreign Assets Control (OFAC).<sup>58</sup>

An excellent example of where auditors could use expert systems in the banking industry is that many banks still use manual procedures to scan large mainframe computer reports to detect suspicious activities. Many small to mid-size banks complain that because costs to develop automated money laundering monitoring systems are so great, they are unable to afford them.<sup>59</sup> During the 1998 Southwest Border Money Laundering Conference, the Bank of America provided a description of how it identifies suspicious, repetitive or incomplete financial transactions that appear to be associated with money laundering. It also originally implemented a procedure to manually scan

---

<sup>57</sup> U.S. Congress, Office of Technology Assessment (OTA), *Information Technologies for Controlling Money Laundering*, OTA-ITC-630 (Washington, DC: U.S. Government Printing Office, September 1995). 53.

<sup>58</sup> OFAC issued regulations that prohibit, in various ways, trade with specific countries, including Cuba, North Korea, Libya, Iraq, the former Yugoslavia, UNTIA (Angola), and Iran. In addition, to countries, individuals are on this list, if they are known to be dealing in illegal activities (drug trafficking, terrorism, etc.)

<sup>59</sup> Banks also cite the U.S. Government's own reports that "laundered money account for approximately 0.05 percent of all wire transfers in the United States." With this in mind, banks believe that the burden of costs to them would greatly out weigh the benefits of any type of system.

mainframe computer reports, but again the procedure was tedious. Subsequently, the Bank developed a monitoring system which automatically downloads "suspicious" data from the mainframe computer. From a daily average of 100,000 transactions, the Bank downloads approximately 3,500 transactions that it considers "suspicious", of which 300 to 500 will be subjected to manual review. The system is designed to eliminate several types of transactions that are deemed as "not suspicious:" bank-to-bank transactions, known corporate entities, individuals exempt from SAR reporting, etc. Of the 300 to 500 reports, the operator of the system then manually scans these transactions creating "Hot Files" of suspect transactions which are used for future comparisons.<sup>60</sup> This centralized system, although considered a great advance, still leaves room for improvement. Only "one individual examiner reviews these transactions nationwide."<sup>61</sup> That suggests that if this person reviews all of these transactions for eight hours a day, with a daily average of 400 reports, then each report is seen for an average of 1.2 minutes. For this reason, it was stated that many banks are between 4 to 6 months behind on reporting.<sup>62</sup> While these systems are quite simple in comparison with FinCEN's system, they are examples of how such systems can be integrated with bank operations.

Each of these systems, has limitations. FinCEN's are much in part due to its own parent agency, the U.S Treasury Department, and how it issued guidance to banks on how they must retain CTR data and in what form. Guidance was provided on the length of time that CTRs were to remain on file within the banks, but the Treasury did not want to dictate in what form or for how long in any particular form. For this reason, data

---

<sup>60</sup> Vaurio, 6.2.1

<sup>61</sup> Unnamed Federal Agent, DrugMARKET Peer Review Meeting, November 1998.

<sup>62</sup> Ibid.

provided to FinCEN is not always easily accessible. For example, the Federal Reserve [Fedwire] retains records on-line for three days, on tape for 180 days, and on microfiche for seven years. Within the private banking industry the problem is even worse. Though bank records originated in electronic form, they are often stored electronically for only a short period of time. Some large banks keep long-term records on microfiche while many smaller banks keep their records in paper form. The various record-keeping and computer systems used to conduct and record bank wire transfers were never intended to be used as monitoring devices. They were designed for quick and reliable processing of large volumes of fund transfers. This mission does not require centralized record-keeping, long-term electronic storage, or quick retrieval of the sort required for law enforcement purposes. Thus when FinCEN requests certain wire records from banks, it does not know what the format will be and analysts and/or investigators must waste valuable time inputting data into FAIS in some form that it will understand.

Partly for this reason, another study was commissioned by the OTA to study how technology, in the form of expert systems, could assist law enforcement in their fight against money laundering. The OTA came up with two recommendations, they were:

- 1) Targeted Access to Wire Transfers for FinCEN, and
- 2) Two-Level Screening and Evaluation.

Targeted Access to Wire Transfers for FinCEN would require banks to provide wire transfer records electronically to FinCEN in response to its specific requests. FinCEN would hold legislatively conferred subpoena power<sup>63</sup> to make such requests on the basis of documented suspicion derived from a confluence of Currency Transaction

---

<sup>63</sup> The automated subpoena is the requirement for Project No. 6 (Digital Bank Subpoena Processor) of the findings from the DrugMARKET Report.

Reports (CTRs) selected by FAIS, law enforcement tips, and link analysis. The CTRs would be analyzed in the context of other government and commercial databases through link analysis. Use of this system would primarily confirm and sharpen existing leads, thus providing additional support to law enforcement investigations and prosecutions. Of course, few new leads would be generated by this system.

Building on the already existing expert system at FinCEN, this new system would target the wire transfer records to be requested. The selection would be based not on information carried on the CTR but on other established grounds. Thus, it would be able to reduce enormously the number of CTRs to be examined. This configuration most closely approximates current law enforcement practice. As a consequence, it is likely to be least objectionable to privacy advocates. Moreover, an "electronic subpoena" direct from FinCEN to the banks would streamline the subpoena process and facilitate timely investigations. Nevertheless, it would require a nearly novel "administrative" subpoena power for a law enforcement agency. This departure from the traditional model of criminal subpoena issued by a grand jury would set a potentially broad precedent. Careful sculpting of the criteria for issuing this subpoena may be able to insulate it from constitutional attack, but affected parties would likely have no opportunity to quash the subpoena. Even so, civil libertarians and privacy advocates may prefer it to other options.

Costs should be moderate for the government and for banks. Such a system would build on systems already in place for money center banks with their electronically retrievable records. While FinCEN's existing systems are more fully utilized, new capacity would be required to store and analyze the increased number of records.

Two-Level Screening and Evaluation would require banks to operate one level of screening of wire transfer traffic using guidelines developed by FinCEN in consultation with banks. Expert systems would be adapted to interface with the banks' own record keeping and retrieval systems. Banks would not select suspicious records *per se* (avoiding the problems of profiling and of sparse message data). Instead, they would eliminate "nonsuspicious" transfers (e.g., those originated by established and well-regulated banks, national and international corporations, and well-known customers).

The remaining, but greatly reduced traffic (perhaps about 25 percent of the total, or 150,000 transfers per day)<sup>64</sup> would be copied and sent to FinCEN where they would be further filtered by the new expert system, to identify suspect subjects and accounts. The suspect records would then be analyzed by FinCEN's link analysis operations (i.e., matched with data from CTRs and from government and commercial databases for contextual information). The primary product would be new leads, but evidentiary support for ongoing investigations would also be generated. The system might not catch multi-bank laundering operations if differences in banks' implementation resulted in different levels of screening.

Costs would be moderate-to-high for banks and high for governments. The system would require a substantial increase in technology for banks to screen transfers. Processing of 150,000 records daily at FinCEN would require major new capacity and human resources. This would be an order of magnitude increase in current workload in spite of the huge reduction in volume of transmissions monitored. As of the date of this

report, neither one of these recommendations has been implemented, due to costs on both the banking industry as well as changes in current federal laws on banking and wire transfers.

Bank auditors using expert systems to assist them with risk analysis and internal control analysis will directly enhance law enforcement anti-money laundering efforts. The new expert systems would evaluate existing EDP systems and identify where controls in the accounting systems lack adequacy and ultimately might suggesting where additional controls might be needed. Donald Watne stated that auditors in the performance of their functions, "not only must be familiar with the basic standards and concepts of auditing, but must also understand the additional standards and concepts specifically applicable to auditing EDP systems".<sup>65</sup>

Among the many different disciplines in the field of accounting, auditing is the most obvious beneficiary from expert systems which can assist in the analysis and evaluation of a bank's controls, performance standards, and operating procedures. Such systems can aid in the study and evaluation of internal control, perform analytical review procedures, interpret their significance, and potentially relieve the problems of "standards overload" by assisting auditors with solutions to complex reporting and disclosure questions. The laundered funds originating from Russia that flowed through the Bank of New York accounts would have been brought to light earlier, if the expert systems would have been used to increase internal controls. The anomalies or distinct patterns that were overlooked by the banks anti-money laundering system would have been flagged and

---

<sup>64</sup> Currently, FinCEN receives approx. 30,000 CTRs. The author sees this five-fold increase as impractical, given that FinCEN cannot handle the workload that it currently has, as noted elsewhere in this report.

<sup>65</sup> Watne, 91.

reported to the internal auditors for further inspection. As with the other systems recommended by OTA, cost appears to be the primary factor limiting the implementation of these systems.

### **Research Process**

Whereas, the second research question in Chapter 3 was intentionally structured, the question which follows allows the interviewees more creative contributions and recommendations to the research.

### **Questions #3**

Can any additional technologies be identified from an auditor, forensic accountant or CFEs professional perspective, which would be viewed as an asset to their work in money laundering cases in the field of banking?

### **Findings**

The majority of respondents stated that some sort of expert system should be designed using a combination of experts in the areas of accounting and law enforcement.<sup>66</sup> The system designed and developed should enhance the detection of "high quality" SAR's. The Principal Investigator/FACFE stated that "The system would be defeating itself if it only created more SARs. You know the old saying, trash in and trash out. A system needs to be developed that can lessen the burden of information

---

<sup>66</sup> Most experts believe that most money laundering could not take place within the U.S. if it were not for the assistance of accountants and lawyers who are familiar with current anti-money laundering laws and various schemes to manipulate funds.

overload." The system should also utilize those items developed by the Banking SAR Algorithm Project. These two items combined with the bank auditors review of the final reports would help highlight anomalies or suspicious activities. The higher quality CTR would then be provided to FinCEN and FAIS for further analysis and review. Any "hits" made by FinCEN could then be followed up with the "electronic/digital subpoena" to establish a case if needed.

The respondents also stated that the system would be greatly enhanced if banks complied with and followed-up with the Know-Your-Customer rules. Auditors could monitor suspect customer transactions over a period of time to permit a determination of whether the customer's actions are truly suspicious and require reporting. The FBI Supervisory Agent stated however, that "the question would then fall back on the integrity of the bank. Would they utilize the expert system *carte blanche* or selectively?" Banks also state that they should not have a "quasi-government or law enforcement role"; they are a business and exist to make profits.

Several respondents stated that if the detection systems were completely automated they could be set to run with the nightly processing of transactions and generate a list of suspicious transactions that would then be followed up by the auditors. This system would be in near real-time as some argue for and would be a great improvement over the current system which requires banks to file CTR within 30 days of the act. Many respondents also felt that each transaction could be reviewed by the system looking for "known suspects, their relatives and known associates"<sup>67</sup>.

---

<sup>67</sup> Dr. Carapezza, interviewed by the author, stated that DARPA also realized that the problem of money laundering is so computationally intensive that it is considered NP Complete. If you have all of the computer power in the world and all of the time you need the problem would still be unsolvable. Therefore, constraints must be placed on the search to highly probable (suspicious) targets.

One respondent stated that the:

"percentage of participation would depend on resources available to be allocated to the manual process of following up on the suspicious transactions generated in the nightly processing. The percentage would also depend on any new regulations, penalties and the degree of related enforcement."<sup>68</sup>

The systems would be used to enhance current investigations, not generate new ones.

The Principal Investigator/FACFE stated that "expert systems could be developed to increase the internal control abilities of banking auditors. Computers and the use of EDP has caused the average auditor to become overwhelmed" when combined with all of the reporting rules required under federal and state laws, federal rules and regulations governing general banking, the rules for GAAP and GAAS, etc. The FBI Supervisory Agent stated that "auditors are generally unaware of how to apply processes, etc. to determine the sources of money" and therefore, require assistance. Therefore, the use of expert systems to develop a check mechanism for banks internal controls would be of great assistance to the auditors.

### Issues

The respondents concurred that the main hurdle for this approach is the cost of purchasing as well as operating these "expert systems". Therefore, if a system could be developed and provided to the banks at no cost, banks would be more likely to accept them. As with the DrugMARKET Projects, if banks could turn these areas of "cost" into "revenue" areas there stands a much better chance that banks would be willing to

---

<sup>68</sup> Respondent No. 1: Forensic Accountant/CFE

implement these proposed systems. If banks were given an incentive to look for money laundering activities, such as a percentage of all funds seized in by asset forfeiture laws, or passing the cost to customers, they would be more willing to assist law enforcement rather than provide the required minimum.

### **Implications and Recommendations**

Expert systems are seen by those in law enforcement and auditing as an asset in the fight against money laundering. This finding must be qualified in several respects. First, the interfaces between expert systems and auditing must be defined, and how best to optimize these processes. Advances in expert systems must constantly be configured to allow for the human-in-the-loop. Second, research and development costs and systems development come at a heavy cost for which there are presently few, if any incentives. And, finally, might the money laundering domain be so complex, that expert system-auditor applications might only make a marginal dent in money laundering detection. One can only speculate from the government and corporate viewpoint, if a heavy commitment in resources brings a return-on-investment. From the viewpoint of those surveyed, the expert system-auditor interface has value.

Respondents made basically the same recommendations as discussed in Chapter 3. That is say, that respondents are in concurrence with contemporary thinking that technology plays an important role in the detection, of money laundering. These respondents did not qualify their answers with discussions of the many shortfalls and limitations these applications may present. To repeat, the concurrence of the respondents is in line with prevailing studies, reports, and recommendations all pointing to increased

technology applications to counter money laundering. Precisely, what systems and at what cost, is a national policy decision.

The role of the auditor and an adjunct to the technological considerations, is an important one. The criticality of the auditor, and the capability of the auditor to perform as a human-in-the-loop, is a significant matter.

## CHAPTER 5

### SUMMARY AND CONCLUSIONS

#### Summary

Law enforcement agencies attempt to track money laundering in order to detect and document an underlying crime. This strategy grew from frustrations over failed attempts to interdict drug trafficking and further increased as the role of money laundering in terrorism, illegal arms trading, and white collar crime was realized. A series of laws gradually criminalized activities related to money laundering, providing new weapons in the anti-laundering fight. Many of these laws have proven ineffective due to the unwillingness of those in the banking industry to do more than the "letter of the law" and those in government that do not wish to impose harsh penalties for non-compliance.

Therefore, law enforcement looks to technology to assist in solving its problem. Most studies have looked at techniques developed in the field of artificial intelligence and have made recommendations that some sort of expert system can be developed, but with unacceptable costs.

Many say that the expert systems should be imposed upon banks, and that the banking industry should pay for the systems. The banking industry however, continues to resist any imposed regulations, stating that banks are in the business to make money and anti-money laundering laws impose costs to a bank each time that it fills out a required report.

It is wishful thinking to expect technology to resolve all of our problems, including money laundering. Our great and modern financial system provides many more criminal opportunities than law enforcement can ever hope to forestall or block even with anti-laundering technology. Therefore, an alliance must be made between those in the law enforcement community and those in the banking industry. Currently, there are agreements between the two. Banks will not knowingly participate in money laundering and will assist law enforcement in every way legally possible. However, the current agreements are not working and therefore, new methods and ideas must be addressed.

This study attempted to continue research beyond the recently derived DrugMARKET findings. Certain extensions, modifications and a change of focus were done in an attempt to develop new findings as well as make recommendations that would provide added value to the investigation and prosecution of money laundering, while at the same time, and advance tools of practice in auditing and forensic accounting.

### **Conclusion**

It is the opinion of this author that there is no easy fix to the money laundering problem that we face. This paper however, has identified what I believe are supporting roles for law enforcement investigators and banking auditors and how they can use technology to assist their detection efforts. The technology identified is state -of-the-art, however, it is not a silver bullet. The technology will not completely halt money laundering activities, but it may assist in closing more cases.

To look at this issue from a Machiavellian point-of-view, the current social and political desire to do away with money laundering is not there. Far too much money is involved. Despite recommendations of various government-funded reports and studies, there has not been a strategic or coherent effort to launch an R&D effort for this purpose. Also, there is an ongoing concern for big government, "Big Brother is Watching" and the "New World Order". Thus, law enforcement's increase in power and at least the perceived view of a government's right to monitor would need to outweigh the individual citizens right to privacy.

The banking industry also resists more regulation along with its additional costs. Unless the government pays for new requirements, allow the banks to receive a portion of seized assets or pass costs off to the consumer, banks will not want to implement such monitoring systems. Libertarian groups argue that the citizen's right to privacy outweighs the government's right to monitor such activities. The average person appears willing to allow some amount of illegal activity to go undetected in order to protect their privacy. Therefore, with the free society that we have come to enjoy as an "inalienable right", the government will never be able to completely control the financial system. Too many individuals, groups, and organizations (both saints or sinners) will resist for practical or principal reasons.

## **ABBREVIATIONS**

ACFE	American College of Forensic Examiners
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
B	Billion
BSA	Bank Secrecy Act
CDTDPO	Counterdrug Technology Development Program Office
CFE	Certified Fraud Examiner
CHIPS	Clearing House for Interbank Payments System
COSO	Committee of Sponsoring Organizations
CPA	Certified Public Accountant
CTR	Currency Transaction Report
CIAS	Customs Artificial Intelligence System
DARPA	Defense Advance Research Projects Agency
DEA	Drug Enforcement Administration
DrugMARKET	Drug Money Analysis, Research and Knowledge Engineering Task
DocEx	Document Exploitation
DoD	Department of Defense
DSS	Digital Support System
EDP	Electronic Data Processing
FA	Forensic Accountant
FBI	Federal Bureau of Investigation

Fedwire	Federal Reserve's electronic funds and securities transfer service
FDIC	Federal Deposit Insurance Corporation
FIAS	Financial Artificial Intelligence System
FinCEN	Financial Crimes Information Network
FRU	Financial Remedies Unit
FW	Standards of Field Work
GAAS	Generally Accepted Auditing Standards
GAAP	Generally Accepted Accounting Practices
GS	General Standards
HIDTA	High Intensity Drug Trafficking Areas
IC	Internal Control
IRS	Internal Revenue Service
IT	Information Technology
MCA	Money Control Act
M	Million
OCR	Optical Character Recognition
OFAC	Office of Foreign Assets Control
ONDCP	Office National Drug Control Policy
OTA	Office of Technology Assessment
R&D	Research and Development
RICO	Racketeer Influenced and Corrupt Organizations Act
SAC	Systems Auditability and Control
SAR	Suspicious Activity Report

SAS	Statements of Auditing Standards
SR	Standards of Reporting
T	Trillion

## APPENDIX A

### DRUGMARKET PROJECT DESCRIPTIONS:

#### **Background**

In October, 1998 the Executive Program, Department of Defense (DoD) Counterdrug Technology Development Program Office (CDTDPO) appointed a panel of experts to study the information handling and processing challenges to money laundering investigators and prosecutors, focusing on information technology (IT) tools and methodologies. This study known as Project DrugMARKET (Drug Money Analysis, Research and Knowledge Engineering Task) was to baseline the state-of-the-art in money laundering investigation capabilities of the field investigator and the prosecutor. The objective was to discover what works and what does not, and how investigations could be conducted better, faster, and cheaper. The study was concluded and issued a final report which documented its findings. The report offered twelve specific recommendations for new technology areas to assist in future investigations and project developments.

The DrugMARKET study provides findings for analysis of the money laundering problem both from the prospective of technology and investigative/prosecutorial needs, but also as it may be viewed valuable by the auditors, forensic accountant or certified fraud examiners specifically those working in the banking industry.

Please review the 12 technologies below and complete the attached questionnaire.

**1. Bank Industry SAR Algorithms Project:** The Bank Secrecy Act (BSA) of 1986, latter amended, authorized the Secretary of the Treasury to require any financial institution, and its employees "to report any suspicious transaction relevant to a possible violation of law or regulation". It requires institutions to file a Suspicious Activity Report (SAR). The Act identifies some eighteen categories of suspicious activity ranging from loan fraud, credit/debit card fraud, and money laundering.

**Requirement:** Increase the number of SARs reported, especially those relating to money laundering. Some financial institutions use automated systems which allow them to identify "suspicious activity", however, many more institutions still use manual paper reports. There exists an opportunity to significantly improve the automated and semi-automated identification process of detecting suspicious transactions by developing more complex algorithms to examine all transactions. Such algorithms could be accompanied by new procedures which would enable law enforcement to provide, real-time data to the banking industry which could more precisely define suspicious activity.

**2. Case Reconstruction Demonstration Project:** During the investigation of a case, the investigative agency develops and maintains a case file(s) which contains all relevant information about the case. When a decision is made by the prosecutor that sufficient evidence exists to charge suspect(s) and proceed with a trial, the case file serves as the foundation for "building" the prosecution. The "knowledge" contained in the case file is usually supplemented by information developed/acquired by the prosecutor, however, this new information may be archived independently of the original "case file". In any event, as the prosecution builds and prosecutes the case, the original case file most often is not the master archive for all information about the case. In addition to grand jury information, further knowledge about suspects/defendants is also uncovered during the trial. After the prosecution phase is terminated, there is generally little feedback to the originating investigative agency. The result is that the original case file no longer is the single, authoritative archive for all of the information related to the case and its subsequent prosecution. The net result: very little, if any, of the intelligence of potential new suspects and money laundering organizations is captured for future use.

**Requirement:** Systematically quantify the case knowledge contained in the originating investigative agency's case file, then quantify the case knowledge developed and acquired during the prosecution phase of the case; and compare the differences between the two files. The result should help identify what information is "lost" or never captured from the investigative agency's perspective. Next, extend the functionality to ensure that the nuances of the prosecutor and support team methods of operation can be documented. Thirdly, define alternative approaches to disseminating the prosecutor's information back to the investigative agency for use on related or future investigations.

**3. Cash Currency Processor:** Law enforcement agents routinely utilize government-provided cash currency during undercover drug operations. After the operation is terminated and suspects are arrested, any cash currency which has been seized can be compared with a list of serial numbers which were recorded prior to the operation. A match of serial numbers may be considered additional evidence against the defendant. Another technique involved an undercover agent who was involved with suspects operating a drug cash stash house; however, the location of the stash house was unknown to the agent. In this operation, the cash counting machine was modified with a tracking device and provided to the suspects in order to track the machine to the stash house.

**Requirement:** Develop an automatic currency counter, with the ability to read the denomination of bills, the number of bills processed and their total value, read serial numbers; copying output results to a database or spreadsheet. Lastly, modify the currency counter and/or the serial number reader so that the device can be located remotely.

**4. Paper Currency Detection Phenomenology Study:** The smuggling of U.S. currency out of the country is a large problem. Most represent the illicit profits of drug traffickers and is a crude form of money laundering. The typical *modus operandi*, is the dense packing of (plastic wrapped and/or metal foil wrapped) batches of bills in hidden locations within vehicles. It is possible to use penetrating x-rays at inspection points (ports of entry/exit) to detect hidden currency; however, there are very few x-ray devices along the U.S. Border and their principal use is for non-intrusive inspection of incoming vehicles, not outbound vehicles.

**Requirement:** Remotely detect bulk U.S. paper currency at ports of entry/exit (along the border, at airports, cargo shipyards), along interstate highways, and packages via the U.S. Mail and other package delivery services.

**5. Currency Serial Number Tracking Concept Study:** Various law enforcement agencies have on occasion recorded the serial numbers of cash paper currency used in law enforcement investigations (see Project 3). Numbers are also recorded for accountability and traceability requirements. Since money is, in essence, a fungible commodity, the traceability of a known "dirty" bill from beyond the immediate confines (both in location and time) of an undercover drug buy operation is unknown. It may be possible to construct operations research scenarios and a model of the movement of "dirty" cash currency into and out of legitimate commercial activities. Such a model could be used to evaluate the potential usefulness of deploying "choke point" currency serial readers at locations such as banks.

**Requirement:** Quantify the utility of centralized databases of "dirty" currency serial numbers within the context of automatic serial number readers/recorders deployed at strategic "choke point" locations within a given geographic area.

**6. Digital Bank Subpoena Processor Project:** Prosecutors routinely prepare subpoenas that direct individuals, organizations or businesses to provide information that is relevant to an investigation. In the case of money laundering such subpoenas frequently are directed to banks. During the preparation of the subpoena, specific items needed must be identified (i.e. the names of individuals, businesses, account numbers, transactions, range of dates). Depending on the complexity of the information requested, the amount of time to locate the data and prepare it for transmission to the requesting legal entity, can vary from days to months. The information provided is troublesome, since it is typically photocopies of original documents. Many times, banks respond with dozens of large boxes filled with individual pieces of paper. In order for the information to provide value to the investigator, each individual piece of paper must be physically examined and processed to retrieve information. The information is then recorded in either a ledger, electronic database or spreadsheet. The process is time consuming and is almost never completed if the volume of paper is too large. At some point however, all of the data provided is processed by the bank and converted to electronic records.

**Requirement:** The requirement is to create a legally acceptable subpoena which directs banks (or other financial institutions) to respond to the subpoena via electronic methods.

**7. Documentation Exploitation (DocEx) and Text Extraction Demonstration:**

Document exploitation (DocEx) is a process that results in tangible information found through the immediate and *post facto* analysis of seized documents such as checks, receipts, handwritten notes, deeds, telephone bills, utility bills, rental agreements, day planner notebooks, etc. The exploitation of such documentary evidence can identify previously unknown persons and associations, operating methods, and assets such as financial accounts, safety deposit boxes, storage sites, and property. At the present time the DocEx process is largely a lengthy, manual, and manpower intensive process, and therefore cost prohibitive for many law enforcement agencies. The net result is that many seized documents are never analyzed.

**Requirement:** Simplify and reduce the amount of time required to complete the DocEx process by incorporating automated information processing. This is a three part task: 1) convert paper based documents to an electronic format, 2) obtain optical character recognition (OCR) process for textual information which converts the "image" of text to digital text, and 3) automate or semiautomate extraction of textual information such as named entities (i.e., addresses, telephone numbers, etc).

**8. Electronic Money Laundering Case Template:** The linkage between the investigator and the prosecutor is crucial to the successful prosecution of a case. Although case files serve as the foundation of that link, the files are generally documentary, in paper form, bulky. As a result, the key elements are difficult to quickly synthesize. Investigations are generally complex, containing detailed inter-related data that can become difficult to easily visualize if the case grows in size and/or duration. The coordination of the investigatory elements of the case and the ultimate transition of the case to prosecutors are typically performed in a manual, non-automated manner. Since investigators lack computer support, supervisors currently spend much of their time searching for, manipulating, and sharing information rather than making investigation related decisions. What is lacking is an infrastructure which portrays everything of significance that is known and unknown about a specific case. This capability would consist of a standardized methodology to achieve situational awareness of a case from the perspective of the investigator, the supervisor, and the prosecutor.

**Requirement:** Development of a standardized methodology and template to achieve situational awareness of a money laundering case from the perspective of the investigator, the supervisor, and the prosecutor, that is scalable and simple. It will utilize complex problem solving algorithms to define simple ways to represent relevant concepts and merge them to generate high quality, tightly coordinated money laundering case awareness.

**9. Money Laundering Data Analysis & Visualization Operational Test and Evaluation:** Many software developers have produced data analysis and visualization tools which are purported to provide enhanced analytic capabilities to money laundering investigations. Some or all of these tools may be able to provide insight into the relationships between and among money laundering data elements, which are currently being overlooked today.

**Requirement.** The requirement is to perform an unbiased evaluation of existing data analysis and visualization tools to assess their effectiveness in money laundering investigations.

**10. Paper Check Imager Processor Project:** Canceled checks contain a significant amount of information useful to an investigator in money laundering cases (i.e. name of payee, and maker, address, dates, amounts, bank name, bank account numbers, and routing numbers for inter-bank processing, endorsing persons/organizations, bank date/time stamps, and various other markings such as hand stamps of logos, etc). Problem: financial institutions often "overprint" their endorsement information on top of other endorsement information. In response to a subpoena, financial institutions provide photocopies (front and back) of the checks, typically through their in-house canceled check processing and archival systems (usually microfiche). Photocopies are sometimes "optically degraded" resulting in difficulty in completing analytic examination of "marks" on the reverse of the checks. Sometimes banks are requested to provide a second copy of the "optically degraded" checks, but the ultimate quality is again limited by the original condition of the check prior to microfiche processing

**Requirement:** Enhance the capability in the exploitation of canceled checks by developing a prototype paper check imaging processor which can be a cost effective replacement for microfiche processing/archive systems. Also, develop advanced image enhancement capabilities, specifically for "marks or stamps" hand or machine printed on the reverse of canceled checks. Endorsements which are "overprinted" should be individually extractable so that the underlying endorsements can be retrieved and possibly image enhanced.

**11. Precision Query in Very Large Databases Study and Proof of Concept:** The investigative software package distributed to Internal Revenue Agents criminal investigation special agents includes remote access capability via computer modem to the commercial Lexis Nexis database. Currently, all major federal law enforcement agencies have access to ChoicePoint's CDB Infotek System which offers a repository of databases with more than 3.5 billion online public records. Agents can use the system to uncover hidden asset ownership, locate individuals and provide leads for criminal and civil investigations.

**Requirement:** Queries into very large databases are very similar to using internet search engines. The problem is that if the query is not bounded (i.e., limited or constrained), then the results of the query may be excessive in number (i.e., sometimes

exceeding 100,000 results). While the data the investigator desires may likely be buried in the results, the sheer volume of results precludes manual review of each result. Therefore the requirement is to assist the investigator in making precision queries that reduce substantially the number of results from each search to a manageable number, for example, hundreds.

**12. Targeting Random Phone Use for Authorized Surveillance:** The basic problem is a bank of pay phones located in some public area (i.e. a train station with 32 phones side-by-side). Law enforcement agents conducting a surveillance on a suspect who approaches a phone bank and randomly picks one of the 32 phones to place a call. The agents are unable to determine, by direct observation, exactly which telephone is being utilized. The dilemma is the inability to know in advance exactly which phone the suspect will use and the accompanying problem of being unable to obtain a court order for wiretap authorization on all 32 phones.

**Requirement:** The technology desired is some sort of electronic shunt which could be installed between the phone bank and the switchbox. The shunt could be remotely activated by an agent who is in direct surveillance of the suspect making the phone call. Therefore, if the suspect selects phone number 3, for instance, the agent could activate the shunt to record that phone call only. What is required is the basic technology to perform such a function and the authorization from a court that such a technical approach would be in compliance with current wiretap limitations.

## APPENDIX B

### INTERVIEW QUESTIONNAIRE:

Name:

Title:

Telephone #:

Agency/Organization:

Years money laundering case experience:

#### Question #1:

Do existing accounting rules and standards of practices have direct application and provide enough utility to auditors in the field of banking during the investigation of money laundering cases?

Comments:

#### Questions #2:

Do the 12 candidate technologies (see attached) developed from the findings of the DrugMarket study team, provide utility to auditors, forensic accountants or Certified Fraud Examiners (CFEs) working money laundering cases in the field of banking?

Rank order (a minimum of 3) on the basis of their utility to the investigation/prosecution of money laundering cases and then rank order (a minimum of 3, unless you feel that none of these apply) on the basis of their utility to forensic accountants/ auditors working such cases. Comment on the top 3 technologies (also if none apply) for auditors/forensic accountants.

	Investigators/ Prosecutors	Auditors/ Forensic Accountants
1. Banking Industry SAR Algorithm	-----	-----
2. Case Reconstruction Demonstration Project	-----	-----
3. Cash Currency Processor	-----	-----
4. Currency Detection Study	-----	-----

- |   |       |  |       |
|---|-------|--|-------|
| 5. Currency Serial Number Tracking                | ----- |  | ----- |
| 6. Digital Bank Subpoena Processor                | ----- |  | ----- |
| 7. Document Exploitation DocEx Project            | ----- |  | ----- |
| 8. Electronic Money Laundering Case Template      | ----- |  | ----- |
| 9. Money Laundering Data Analysis & Visualization | ----- |  | ----- |
| Operational Test and Evaluation                   |       |  |       |
| 10. Paper Check Imaging Processor                 | ----- |  | ----- |
| 11. Precision Query - Very Large Data Bases       | ----- |  | ----- |
| 12. Targeting Random Phone Use                    | ----- |  | ----- |

Comments:

**Questions #3:**

Can any additional technologies be identified from an auditor, forensic accountant or CFEs professional perspective, which would be viewed as an asset to their work in money laundering cases in the field of banking?

Comments:

Thank you for time and effort in participating in this study. If you would like a copy of the final report, please indicate.

\_\_\_\_\_Y      \_\_\_\_\_N

## APPENDIX C

### RESPONDENTS:

Several respondents provided information with regards to this study on a confidential basis. Upon their request I have omitted the names of all of the respondents who completed the questionnaire. However, the names will be provided to the Directed Study Adviser for possible verification purposes.

Respondent #1: Former Chief of Drug & Currency Crimes, Internal Revenue Service  
IRS Criminal Investigation Division (Retired), Forensic Accountant,  
Enrolled Agent, Certified Fraud Examiner. 15 years.  
(Referred to as: Forensic Accountant/CFE)

Respondent #2: Forensic Criminologist, Principal Investigator on Project DrugMARKET  
Consultant to National Institute of Justice, and National White Collar  
Crime Center. Life Fellow, American College of Forensic Examiners  
(Referred to as: Principal Investigator /FACFE). 5 years.

Respondent #3: Financial Analyst Coordinator, New Jersey Division of Criminal Justice  
Former President, International Association of Law Enforcement  
Intelligence Analysts, Certified Criminal Analyst & Certified Fraud  
Examiner. 16 years.  
(Referred to as: State Official/CFE)

Respondent #4: Bank Examiner, Federal Deposit Insurance Corporation,  
Former IRS Tax Compliance Officer. 5 years.  
(Referred to as: Federal Bank Examiner)

Respondent #5: Former FBI Supervisory Agent,  
Asian Organized Crime & La Cosa Nostra. 18 years.  
(Referred to as: FBI Supervisory Agent)

Respondent #6: Information Services Supervisor, National White Collar Crime Center  
Member, International Association of Law Enforcement Intelligence  
Analysts. 7 years.  
(Referred to as: White Collar Crime Analyst)

## BIBLIOGRAPHY

- American Institute of Certified Public Accountants, *Statements of Auditing Standards (SAS) No. 55 (as revised by SAS No. 78)*.
- Beckman, Robert L., "The Phoenix Financial Task Force Southwest Border HIDTA." Arlington, VA: Science Applications International Corporation, 1999. Photocopied.
- Bortne, Mark. *Cyberlaundering: Anonymous Digital Cash and Money Laundering*. University of Miami. Florida, on-line.  
[www.law.miami.edu/~froomkin/seminar/papers/bortner.htm](http://www.law.miami.edu/~froomkin/seminar/papers/bortner.htm)
- Colbert, Janet and Paul Bowen. *A Comparison of Internal Controls: CobiT, SAC, COSO and SAS55/78*, Information Systems Audit and Control Association, 1999.  
[www.isaca.org/bkr\\_cbt3.htm](http://www.isaca.org/bkr_cbt3.htm)
- Ehlers, Scott. "In Focus: Drug Trafficking and Money Laundering" U.S. Foreign Policy 3, no. 16 (1998)
- The American Heritage Dictionary of the English Language*, Boston, MA: Houghton Mifflin Company, 1981.
- U.S. Congress, General Accounting Office, "FinCEN Needs to Better Manage Bank Secrecy Act Civil Penalty Cases", (Washington, DC: U.S. Government Printing Office, (1998).
- U.S. Congress, Office of Technology Assessment, *Information Technologies for Office Control of Money Laundering*, OTA-ITC-630, (Washington, DC: U.S. Government Printing Office, (1995).
- U.S. Department of State, Bureau for International Narcotics and Law Enforcement Affairs, *International Narcotics Control Strategy Report, 1998*. Washington, DC, 1999.
- U.S. Department of State, Testimony before the House Committee on Banking and Financial Services, *Combating Money Laundering*. Jonathan Winer. Washington, DC, 1998.
- U.S. Department of Treasury, Financial Crimes Enforcement Network. *Strategic Plan (1997-2002)*, Vienna, VA.
- Vaurio, David., "Project DrugMARKET Interim Final Report." Arlington, VA: VA: Science Applications International Corporation, 1999. Photocopied.

Watney, Donald A., and Peter B. Turney. *Auditing EDP Systems*. New Jersey: Prentice Hall, 1990

Whittington, O. Ray, and Kurt Pany. *Principles of Auditing Articles*. Chicago: Irwin, 1995

Williams, Phil. "Money Laundering" *Criminal Organizations* 10, no.4, University of Chicago, Illinois (1995): 18-26